GFI Product Manual

GFI MailEssentials™

Administrator Guide

GFI®

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.

Windows, Exchange, IIS, .NET, Internet Explorer, Outlook, SQL Server and Microsoft are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All product and company names herein may be trademarks of their respective owners.

GFI MailEssentials is copyright of GFI SOFTWARE Ltd. - 1999-2012 GFI Software Ltd. All rights reserved.

Document Version: 1.5.0

Last updated (month/day/year): 06/03/2013

Contents

1 Introduction **14**

1.1 About this manual 14
1.2 Terms and conventions used in this manual 15
1.3 Licensing 15

2 About GFI MailEssentials **16**

2.1 GFI MailEssentials components 16
2.1.1 GFI MailEssentials scan engine 16
2.1.2 GFI MailEssentials web interface 16
2.1.3 GFI MailEssentials Email Management console 16
2.1.4 GFI MailEssentials Switchboard 16
2.2 Inbound mail filtering 18
2.3 Outbound mail filtering 18
2.4 Email scanning and filtering engines 19
2.4.1 Malicious emails' scanning 19
2.4.2 Content filtering engines 19
2.4.3 Anti-spam filtering engines 19
2.4.4 Filters running at SMTP level 20
2.4.5 Other engines 20
2.5 Typical deployment scenarios 21
2.5.1 Installing directly on Microsoft® Exchange server 21
2.5.2 Installing on an email gateway or relay/perimeter server 21

3 Installation **24**

3.1 System requirements 24
3.1.1 Hardware requirements 24
3.1.2 Processor 24
3.1.3 Available Memory (RAM) 24
3.1.4 Free Disk Space 24
3.1.5 Software requirements 25
3.1.6 Antivirus and backup software 26
3.1.7 Firewall port settings 27
3.2 Pre-installation actions 28
3.2.1 Installing on the Microsoft® Exchange server 28
3.2.2 Installing on an email gateway or relay/perimeter server 28
3.3 Installation procedure 32
3.3.1 Important notes 32
3.3.2 Running the installation wizard 33
3.3.3 Post-Installation Wizard 36
3.4 Upgrading a previous version 40
3.4.1 Upgrade Procedure 40
3.5 Post-Install actions 41
3.5.1 Add engines to the Windows DEP Exception List 42
3.5.2 Test your installation 43

4 Monitoring status **45**

4.1 Dashboard 45
4.1.1 Status and statistics 46
4.1.2 Email processing logs 49
4.1.3 Antivirus and anti-spam engine updates 51
4.1.4 POP2Exchange activity 52
4.2 Reports 52
4.2.1 Enabling/Disabling reporting 52
4.2.2 Generating a report 53
4.2.3 Custom reports 56
4.2.4 Generating custom reports 57
4.2.5 Deleting custom reports 57
4.2.6 Searching the reporting database 57
4.2.7 Configuring reporting database 58

5 User Actions 62

5.1 Personal Whitelist and Blocklist 62
5.2 Quarantine Search 64
5.2.1 Using the Quarantine Search 65

6 Email Security 68

6.1 Virus Scanning Engines 68
6.1.1 Vipre 68
6.1.2 BitDefender 72
6.1.3 Kaspersky 76
6.1.4 Norman 79
6.1.5 McAfee 84
6.2 Information Store Protection 88
6.2.1 Information Store Scanning 88
6.2.2 VSAPI Settings 89
6.3 Trojan and Executable Scanner 91
6.3.1 Configuring the Trojan & Executable Scanner 91
6.4 Email Exploit Engine 94
6.4.1 Configuring the Email Exploit Engine 94
6.4.2 Enabling/Disabling Email Exploits 97
6.5 HTML Sanitizer 97
6.5.1 Configuring the HTML Sanitizer 98
6.5.2 HTML Sanitizer Whitelist 98
6.5.3 HTML Santizer Domain\IP Exclusions 99

7 Anti-Spam 101

7.1 Anti-Spam filters 101
7.1.1 SpamRazer 102
7.1.2 Anti-Phishing 105
7.1.3 Directory Harvesting 107
7.1.4 Email blocklist 110
7.1.5 IP DNS Blocklist 112
7.1.6 URI DNS Blocklist 114

7.1.7 Sender Policy Framework 115
7.1.8 Anti-Spoofing 117
7.1.9 Greylist 119
7.1.10 Header Checking 121
7.1.11 Spam Keyword Checking 124
7.1.12 Bayesian Analysis 128
7.1.13 Whitelist 130
7.1.14 New Senders 134
7.2 Spam Actions - What to do with spam emails 135
7.2.1 Configuring Spam Actions 136
7.3 Sorting anti-spam filters by priority 138
7.4 Spam Digest 139
7.4.1 Configuring spam digests - Administrator spam digest 139
7.4.2 Configuring spam digests - Recipient spam digest 140
7.5 Anti-Spam settings 142
7.5.1 Log file rotation 143
7.5.2 Anti-Spam Global Actions 143
7.5.3 DNS Server Settings 144
7.5.4 Remote Commands 145
7.5.5 Perimeter SMTP Server Settings 148
7.6 Public Folder Scanning 149
7.6.1 Enabling Public Folder Scanning 149
7.6.2 Using Public folder scanning 153

8 Content Filtering 156

8.1 Keyword Filtering 156
8.1.1 Creating a Keyword Filtering rule 157
8.1.2 Enabling/disabling Rules 162
8.1.3 Removing content filtering rules 162
8.1.4 Modifying an existing rule 162
8.1.5 Changing rule priority 162
8.2 Attachment Filtering 163
8.2.1 Creating an Attachment Filtering rule 163
8.2.2 Enabling/disabling rules 168
8.2.3 Removing attachment rules 169
8.2.4 Modifying an existing rule 169
8.2.5 Changing the rule priority 169
8.3 Advanced Content Filtering 169
8.3.1 Creating Advanced Content Filtering rules 169
8.3.2 Removing Rules 173
8.3.3 Enabling/Disabling Rules 173
8.3.4 Sorting Rules 174
8.4 Decompression Engine 174
8.4.1 Configuring the decompression engine filters 174
8.4.2 Enable/disable decompression filters 179

9 Quarantine 180

9.1 Important Notes 180

9.2 Searching the quarantine 180
9.3 Search Folders 185
9.3.1 Default Search Folders 185
9.3.2 Creating, editing and removing Custom Search Folders from Searches 187
9.3.3 Using the Search Folders node to auto-purge quarantined emails 187
9.4 Working with Quarantined emails 187
9.4.1 Viewing quarantined emails 188
9.4.2 Approving Quarantined Emails 189
9.4.3 Permanently Delete Quarantined Emails 190
9.5 Quarantine RSS Feeds 190
9.5.1 Enabling Quarantine RSS Feeds 191
9.5.2 Subscribing to Quarantine RSS feeds 192
9.5.3 Securing access to the GFI MailEssentials Quarantine RSS feeds 192
9.6 Quarantine Options 192
9.6.1 Spam Options 192
9.6.2 Malware Options 195
9.7 Quarantine Store Location and Public URL 198

10 Email Management 201

10.1 Disclaimers 201
10.1.1 Configuring Disclaimers 201
10.1.2 Disabling and enabling disclaimers 205
10.2 Auto-Replies 205
10.2.1 Configuring auto-replies 206
10.3 List Server 208
10.3.1 Creating a newsletter or discussion list 208
10.3.2 Using Newsletters/Discussions 210
10.3.3 Configuring advanced newsletter/discussion list properties 211
10.4 Mail Monitoring 215
10.4.1 Enabling/Disabling email monitoring 215
10.4.2 Configure email monitoring 216

11 General Settings 219

11.1 Administrator email address 219
11.2 Enabling/Disabling scanning modules 219
11.3 Proxy settings 221
11.4 Local domains 222
11.5 Managing local users 222
11.5.1 GFI MailEssentials installed in Active Directory mode 223
11.5.2 GFI MailEssentials installed in SMTP mode 223
11.6 SMTP Virtual Server bindings 223
11.6.1 Binding GFI MailEssentials to another other SMTP Virtual Server. 224
11.7 Version information 224
11.8 Patch Checking 225
11.9 Access Control 225

12 Miscellaneous topics 227

12.1 Virtual directory names 227

12.2 User interface mode ... 227
12.2.1 IIS Security Settings ... 229
12.3 Failed emails ... 231
12.3.1 Reprocessing legitimate emails that fail ... 232
12.3.2 Failed emails notifications ... 232
12.4 Tracing ... 233
12.5 POP2Exchange - Download emails from POP3 server ... 235
12.5.1 Configuring POP3 downloader ... 235
12.5.2 Configure dial up connection options ... 237
12.6 Moving spam email to user's mailbox folders ... 238
12.6.1 Microsoft® Exchange Server 2003 ... 238
12.6.2 Microsoft® Exchange 2007/2010 ... 240
12.7 Move spam to Exchange 2010 folder ... 240
12.8 Synchronizing configuration data ... 241
12.8.1 Anti-spam synchronization agent ... 241
12.8.2 Exporting and importing settings manually ... 246
12.8.3 Export/Import settings via command line ... 249
12.9 Disabling email processing ... 252
12.10 Email backup before and after processing ... 253
12.11 Remoting ports ... 254
12.12 Monitoring Virus Scanning API ... 255
12.12.1 Performance counter in Windows 2003 Server ... 256
12.12.2 Performance counter in Windows 2008 Server ... 256
12.12.3 Performance monitor counters ... 258

13 Troubleshooting and support ... 260

13.1 Introduction ... 260
13.2 Common issues ... 260
13.3 Scanning engines & filters ... 262
13.4 Email Management ... 263
13.5 GFI SkyNet ... 264
13.6 Web Forum ... 264
13.7 Request technical support ... 264
13.8 Documentation ... 264

14 Appendix 1 - Bayesian Filtering ... 265

14.0.1 Training the Bayesian Analysis filter ... 266

15 Appendix 2 - Lotus Domino ... 269

15.1 Lotus Domino incompatibilities ... 269
15.1.1 Internal memos/emails are not scanned ... 269
15.1.2 GFI MailEssentials List Server will not work with Lotus Domino ... 269
15.2 GFI MailEssentials Installation Guide for Lotus Domino ... 269
15.2.1 Installing GFI MailEssentials ... 269
15.2.2 Set up DNS/Router Firewall ... 270
15.2.3 Configuring Lotus Domino to send outbound emails through GFI MailEssentials ... 271
15.2.4 Lotus Domino LDAP Settings ... 272

15.3 Lotus Domino Anti Spam Folder Configuration 273
15.4 GFI MailEssentials Configuration 276

16 Appendix 3 - Microsoft® Exchange 2003 Clusters 278

16.1 Installing GFI MailEssentials in a cluster environment 278
16.2 Uninstalling GFI MailEssentials in a cluster enviornment 279

17 Glossary 280

18 Index 287

List of Figures

Screenshot 1: Specifying administrator's email address and license key 34
Screenshot 2: SMTP server and virtual directory details 34
Screenshot 3: DNS Server settings 36
Screenshot 4: Proxy settings 37
Screenshot 5: Inbound email domains 37
Screenshot 6: SMTP Server settings 38
Screenshot 7: Selecting the default anti-spam action to use 39
Screenshot 8: Creating a test rule on Keyword filtering 43
Screenshot 9: Test email blocked by Test rule 44
Screenshot 10: The GFI MailEssentials Dashboard 46
Screenshot 11: The GFI MailEssentials Services 47
Screenshot 12: Quarantine statistics 47
Screenshot 13: Dashboard charts 48
Screenshot 14: Email processing logs 49
Screenshot 15: Email processing logs filter 50
Screenshot 16: Virus scanning engines updates 51
Screenshot 17: POP2Exchange log 52
Screenshot 18: Creating a report 53
Screenshot 19: Emails blocked graph report 55
Screenshot 20: Searching the reporting database 57
Screenshot 21: Reports database search results 58
Screenshot 22: Configuring a Microsoft® Access database backend 59
Screenshot 23: Configuring SQL Server Database backend 60
Screenshot 24: GFI MailEssentials logged on as a user 63
Screenshot 25: Personal Whitelist\Blocklist 64
Screenshot 26: GFI MailEssentials logged on as a user 65
Screenshot 27: Quarantine Search 66
Screenshot 28: Quarantine Search Results 67
Screenshot 29: Vipre configuration 69
Screenshot 30: Virus scanning engine actions 70
Screenshot 31: Virus scanning engine updates 71
Screenshot 32: BitDefender configuration 72
Screenshot 33: Virus scanning engine actions 73
Screenshot 34: Virus scanning engine updates 75
Screenshot 35: Kaspersky configuration 76
Screenshot 36: Virus scanning engine actions 77
Screenshot 37: Virus scanning engine updates 78
Screenshot 38: Norman configuration 80

Screenshot 39: Virus scanning engine actions 81
Screenshot 40: Virus scanning engine updates 83
Screenshot 41: McAfee configuration 84
Screenshot 42: Virus scanning engine actions 85
Screenshot 43: Virus scanning engine updates 87
Screenshot 44: Information Store Protection node 89
Screenshot 45: VSAPI Settings 90
Screenshot 46: Trojan and Executable Scanner: General Tab 91
Screenshot 47: Virus scanning engine updates 93
Screenshot 48: Email Exploit configuration 94
Screenshot 49: Virus Scanning Engine: Configuration page (Actions Tab) 95
Screenshot 50: Virus scanning engine updates 96
Screenshot 51: Email Exploit List 97
Screenshot 52: HTML Sanitizer configuration page 98
Screenshot 53: HTML Sanitizer Whitelist page 99
Screenshot 54: Domain\IP Exclusions 100
Screenshot 55: SpamRazer Properties 103
Screenshot 56: SpamRazer Updates tab 104
Screenshot 57: Anti-Phishing options 106
Screenshot 58: Directory Harvesting page 108
Screenshot 59: Email blocklist 110
Screenshot 60: Personal blocklist 112
Screenshot 61: IP DNS Blocklist 113
Screenshot 62: URI DNS Blocklist 114
Screenshot 63: Enable and configure the Sender Policy Framework 116
Screenshot 64: GFI MailEssentials Anti-Spoofing filter 118
Screenshot 65: Email Exclusions 120
Screenshot 66: Header checking options 122
Screenshot 67: Language Detection 124
Screenshot 68: Spam Keyword checking properties 126
Screenshot 69: Bayesian analysis properties 129
Screenshot 70: Whitelist tab 132
Screenshot 71: Personal whitelist 133
Screenshot 72: New Senders General tab 134
Screenshot 73: New Senders Exceptions 135
Screenshot 74: Anti-spam actions 136
Screenshot 75: Assigning filter priorities 139
Screenshot 76: Spam digest properties/Administrator spam digest 140
Screenshot 77: Recipient spam digest 141
Screenshot 78: Spam digest recipient list 142

Screenshot 79: Log file rotation 143
Screenshot 80: Global actions 144
Screenshot 81: DNS server settings 145
Screenshot 82: Perimeter SMTP Server settings 148
Screenshot 83: Content Filtering: Body Tab - setting conditions 158
Screenshot 84: Content Filtering: Body Tab- configuring other options 159
Screenshot 85: Content Filtering: Users/Folders Tab 161
Screenshot 86: Add users to a Content Filtering rule 161
Screenshot 87: Attachment Filtering: General Tab 164
Screenshot 88: Attachment Filtering: Actions Tab 166
Screenshot 89: Content Filtering: Users/Folders Tab 167
Screenshot 90: Add users to a Content Filtering rule 168
Screenshot 91: Adding a new Advanced Content Filtering rule 170
Screenshot 92: Actions Tab 171
Screenshot 93: Content Filtering: Users/Folders Tab 172
Screenshot 94: Add users to a Content Filtering rule 173
Screenshot 95: Decompression engine checks 174
Screenshot 96: Malware and Spam Search Area 181
Screenshot 97: Malware and Spam Search Area 182
Screenshot 98: Spam Only search area 184
Screenshot 99: Default and custom search folders 185
Screenshot 100: Default search folders 186
Screenshot 101: Search Results 188
Screenshot 102: Quarantined Items details 189
Screenshot 103: Quarantine RSS feeds 191
Screenshot 104: Spam Options - General Options tab 193
Screenshot 105: Spam Options - User Settings tab 194
Screenshot 106: Quarantine Mode 196
Screenshot 107: Nonexistent Recipients 197
Screenshot 108: Quarantine Store location and Public URL 199
Screenshot 109: Choose Disclaimer type 201
Screenshot 110: New Disclaimer general properties 202
Screenshot 111: HTML Disclaimer 203
Screenshot 112: HTML disclaimer editor 203
Screenshot 113: Plain text disclaimer 204
Screenshot 114: Creating a new auto reply 206
Screenshot 115: Auto-reply properties 206
Screenshot 116: Variables dialog 207
Screenshot 117: Creating a new list 209
Screenshot 118: List footer properties 211

Screenshot 119: Setting permissions to the newsletter 212
Screenshot 120: Entering subscribers to the newsletter 214
Screenshot 121: Enable or disable email monitoring 215
Screenshot 122: Add Mail Monitoring rule 216
Screenshot 123: Configuring email monitoring 216
Screenshot 124: Creating an exception 217
Screenshot 125: Specifying the administrator's email address 219
Screenshot 126: Scanning Manager 220
Screenshot 127: Updates server proxy settings 221
Screenshot 128: Local Domains list 222
Screenshot 129: Version Information page 224
Screenshot 130: Checking for product patches 225
Screenshot 131: Access control settings 226
Screenshot 132: GFI MailEssentials Switchboard - UI Mode 228
Screenshot 133: IIS Security - ACL tab 230
Screenshot 134: IIS Security - Authentication tab 231
Screenshot 135: Enabling Failed emails notification 233
Screenshot 136: Configuring Tracing options 234
Screenshot 137: The GFI MailEssentials POP3 downloader 235
Screenshot 138: Adding a POP3 mailbox 236
Screenshot 139: Dial-up options 237
Screenshot 140: Configuring when to pick up email 238
Screenshot 141: Configuring a master server 244
Screenshot 142: Configuring a slave server 245
Screenshot 143: Configuration Export/Import Tool 247
Screenshot 144: Exporting settings via command line 250
Screenshot 145: Importing settings via command line 251
Screenshot 146: The GFI MailEssentials Switchboard: Troubleshooting 252
Screenshot 147: The GFI MailEssentials Switchboard: Troubleshooting 253
Screenshot 148: Changing Remoting ports 255
Screenshot 149: Adding VSAPI performance monitor counters in Windows 2008 Server 257
Screenshot 150: Monitoring Virus Scan Files Scanned in Windows Server 2008 Performance Monitor 258
Screenshot 151: Active Directory selection 270
Screenshot 152: Verifying the MX record of the DNS 271
Screenshot 153: Lotus Domino Administrator - click Configurations option. 271
Screenshot 154: Click Edit Configuration 272
Screenshot 155: Lotus Domino LDAP Settings 272
Screenshot 156: Enable Anonymous Authentication 273
Screenshot 157: Create a new database 274
Screenshot 158: Load convert result 274

Screenshot 159: Copy to the clipboard a link to the current application 275
Screenshot 160: Include all public and other users' folders when a folder list is requested 275
Screenshot 161: New mail-in database 276
Screenshot 162: Enable Public Folder Scanning 277

1 Introduction

1.1 About this manual

The scope of this Administrator Guide is to help you install, run, configure and troubleshoot GFI MailEssentials on your network. The table below describes the contents of this guide.

Chapter	Description
About	» The components and tools that make up GFI MailEssentials » How inbound and outbound mail scanning works » Overview of the engines that protect your mail system » Typical deployment scenarios For more information, refer to About GFI MailEssentials (page 16).
Installation	» The various environments and email infrastructures supported by GFI MailEssentials » Product prerequisites applicable to your network » Prepare your environment for product installation » Guides you through the installation and upgrade procedures » Walks you through the key steps needed to get the product running on default settings. » Test installation and run the product. For more information, refer to Installation (page 24).
Monitoring status	» How to use the Dashboard to monitor status of GFI MailEssentials in real time » How to generate mail usage statistical and graphical reports For more information, refer to Monitoring status (page 45).
User Actions	Explains what domain users (not domain administrators) can do with GFI MailEssentials » Configuring personal whitelists and blocklists » Maintaining quarantined emails For more information, refer to User Actions (page 62).
Email Security	Explains how to configure anti-malware scanning engines For more information, refer to Email Security (page 68).
Anti-Spam	» How to configure anti-spam filters » What to do with emails identified as spam » Sorting the scanning order by filter priority » General anti-spam settings » How users classify emails directly from their mailbox (Public Folder Scanning) For more information, refer to Anti-Spam (page 101).
Content Filtering	Describes how to configure engines that scan email content For more information, refer to Content Filtering (page 156).
Quarantine	Describes how administer and use the GFI MailEssentials Quarantine. For more information, refer to Quarantine (page 180).

Chapter	Description
Email Management	How to use the tools in the Email Management Tools console » Disclaimers » Auto-replies » List server » Email Monitoring For more information, refer to Email Management (page 201). **NOTE:** From the Email Management console you can also access the Pop2Exchange feature. For more information, refer to POP2Exchange - Download emails from POP3 server (page 235).
General Settings	Describes how to customize general settings for your environment. For more information, refer to General Settings (page 219).
Miscellaneous	Explains various functions and tools that can be used to manage GFI MailEssentials. For more information, refer to Miscellaneous topics (page 227).
Troubleshooting	This chapter describes how to resolve common issues encountered when using GFI MailEssentials. For more information, refer to Troubleshooting and support (page 260).

1.2 Terms and conventions used in this manual

Term	Description
	Additional information and references essential for the operation of GFI MailEssentials.
	Important notifications and cautions regarding potential issues that are commonly encountered.
>	Step by step navigational instructions to access a specific function.
Bold text	Items to select such as nodes, menu options or command buttons.
Italics text	Parameters and values that you must replace with the applicable value, such as custom paths and file names.
`Code`	Indicates text values to key in, such as commands and addresses.

For any technical terms and their definitions as used in this manual, refer to the Glossary chapter.

1.3 Licensing

Information on licensing is available on:

http://go.gfi.com/?pageid=ME_adminManualEN

For information on how GFI MailEssentials counts license use, refer to:

http://go.gfi.com/?pageid=ME_RetrieveAndCountUsers

2 About GFI MailEssentials

Topics in this chapter:

2.1 GFI MailEssentials components 16

2.2 Inbound mail filtering 18

2.3 Outbound mail filtering 18

2.4 Email scanning and filtering engines 19

2.5 Typical deployment scenarios 21

2.1 GFI MailEssentials components

2.1.1 GFI MailEssentials scan engine

The GFI MailEssentials scan engine analyzes the content of inbound, outbound and internal emails using a number of engines and filters. The result of the analysis identifies whether an email is to be blocked or allowed.

NOTE

When installing GFI MailEssentials on Microsoft® Exchange server 2003, it scans the Microsoft® Exchange information store. If installed on a Microsoft® Exchange Server 2007/2010 machine with Hub Transport and Mailbox Server Roles, it will also analyze internal emails.

2.1.2 GFI MailEssentials web interface

Through the GFI MailEssentials web interface, you can:

- Monitor email scanning activity
- Manage scanning and filtering engines
- Review and process quarantined emails
- Generate reports

2.1.3 GFI MailEssentials Email Management console

Configure and manage:

- Auto-replies
- Disclaimers
- Newsletters
- Discussion lists
- Mail Monitoring
- POP2Exchange

2.1.4 GFI MailEssentials Switchboard

Use the GFI MailEssentials Switchboard to configure:

- How to launch the GFI MailEssentials user interface
- Set Virtual Directory names for the web interface and RSS
- Configure a number of other advanced options used for troubleshooting purposes
- Enable/Disable email processing
- Enable/Disable tracing
- Setting email backups before and after processing
- Setting Quarantine Store location and Quarantine Public URL
- Specifying user account for the 'Move to Exchange Folder' settings
- Specifying Remoting Ports
- Enable/Disable failed mail notifications

2.2 Inbound mail filtering

Inbound mail filtering is the process through which incoming emails are scanned and filtered before delivery to users.

Inbound emails are routed to GFI MailEssentials and processed as follows:

1. SMTP level filters (Directory Harvesting and Greylist) can be executed before the email body is received.
2. The email is scanned by the malware and content filtering engines. Any email that is detected as containing malware is processed according to the actions configured. If an email is considered as safe, it then goes to the next stage.
3. The email is checked to see if it is addressed to a list in the list server. If the email matches a list, it will be processed by the list server.
4. The incoming email is filtered by the anti-spam filters. Any email that fails a spam filter check is processed as configured in the anti-spam actions. If an email goes through all the filters and is not identified as spam, it then goes to the next stage.
5. If configured, auto-replies are next sent to the sender.
6. If configured, email monitoring is next executed and the appropriate actions taken.
7. Email is next checked by the New Senders filter.
8. If email is not blocked by any scanning or filtering engine, it is sent to the user's mailbox.

2.3 Outbound mail filtering

Outbound mail filtering is the process through which emails sent by internal users are processed before sending them out over the Internet.

When sending an outbound email, this is routed to GFI MailEssentials and processed as follows:

1. The email is scanned by the malware and content filtering engines. Any email that is detected as containing malware is processed according to the actions configured. If an email is considered as safe, it then goes to the next stage.
2. Remote commands check and execute any remote commands in email, if any are found. If none are found, email goes to the next stage.
3. If configured, the applicable disclaimer is next added to the email.

4. If configured, email monitoring is next executed and the appropriate actions taken.
5. If enabled, Auto Whitelist adds the recipients' email addresses to the auto-whitelist. This automatically enables replies from such recipients to go to the sender without being checked for spam.
6. Email is sent to the recipient.

2.4 Email scanning and filtering engines

GFI MailEssentials contains a number of scanning and filtering engines to prevent malicious emails, spam and other unwanted emails from reaching domain users.

2.4.1 Malicious emails' scanning 19

2.4.2 Content filtering engines 19

2.4.3 Anti-spam filtering engines 19

2.4.4 Filters running at SMTP level 20

2.4.5 Other engines 20

2.4.1 Malicious emails' scanning

The following engines scan and block emails containing malicious content.

Email scanning engine	Description
Virus Scanning Engines	GFI MailEssentials uses multiple antivirus engines to scan inbound, outbound and internal emails for the presence of viruses. GFI MailEssentials ships with Vipre and BitDefender Virus Scanning Engines. You can also acquire a license for Norman, Kaspersky & McAfee.
Information Store Protection	When GFI MailEssentials is installed on the Microsoft® Exchange server machine, Information Store Protection allows you to use the Virus Scanning Engines to scan the Microsoft® Exchange Information Store for viruses.
Trojan & executable scanner	The Trojan and Executable Scanner analyzes and determines the function of executable files attached to emails. This scanner can subsequently quarantine any executables that perform suspicious activities (such as Trojans).
Email exploit engine	The Email Exploit Engine blocks exploits embedded in an email that can execute on the recipient's machine either when the user receives or opens the email.
HTML Sanitizer	The HTML Sanitizer scans and removes scripting code within the email body and attachments.

2.4.2 Content filtering engines

The following engines scan the content of emails, checking for parameters matching configured rules.

Email scanning engine	Description
Keyword Filtering	Keyword Filtering enables you to set up rules that filter emails with particular keywords or a combination of keywords in the body or subject of the email.
Attachment Filtering	Attachment Filtering allows you to set up rules to filter what types of email attachments to allow and block on the mail server.
Decompression engine	The Decompression engine extracts and analyzes archives (compressed files) attached to an email.
Advanced Content Filtering	Advanced Content filtering enables scanning of email header data and content using advanced configurable search conditions and regular expressions (regex).

2.4.3 Anti-spam filtering engines

The following engines scan and block spam emails.

FILTER	DESCRIPTION	ENABLED BY DEFAULT
SpamRazer	An anti-spam engine that determines if an email is spam by using email reputation, message fingerprinting and content analysis.	Yes
Anti-Phishing	Blocks emails that contain links in the message body pointing to known phishing sites or if they contain typical phishing keywords.	Yes
Directory Harvesting	Directory harvesting attacks occur when spammers try to guess email addresses by attaching well known usernames to your domain. The majority of the email addresses are non-existent.	Yes (only if GFI MailEssentials is installed in an Active Directory environment)
Email Blocklist	The Email Blocklist is a custom database of email addresses and domains from which you never want to receive emails.	Yes
IP DNS Blocklist	IP DNS Blocklist checks the IP address of the sending mail server against a public list of mail servers known to send spam.	Yes
URI DNS Blocklist	Stops emails that contain links to domains listed on public Spam URI Blocklists.	Yes
Sender Policy Framework	This filter uses SPF records to stop email sent from forged IP addresses by identifying if the sender IP address is authorized.	No
Anti-Spoofing	Checks emails received with a sender email address claiming to originate from your own domain against a list of IP addresses by GFI MailEssentials. If the sender IP address is not on the list of own-domain server IP addresses, email is blocked.	No
Header Checking	The Header Checking filter analyses the email header to identify spam emails.	Yes
Spam Keyword Checking	This filter enables the identification of Spam based on keywords in the email being received.	No
Bayesian analysis	An anti-spam filter that can be trained to accurately determine if an email is spam based on past experience.	No

2.4.4 Filters running at SMTP level

The following engines scan and block emails during SMTP transmission before the email is received.

FILTER	DESCRIPTION	ENABLED BY DEFAULT
Directory Harvesting	Directory harvesting attacks occur when spammers try to guess email addresses by attaching well known usernames to your domain. The majority of the email addresses are non-existent.	No
Greylist	The Greylist filter temporarily blocks incoming emails received from unknown senders. Legitimate mail systems typically try to send the email after a few minutes; spammers simply ignore such error messages.	No

2.4.5 Other engines

The following engines help to identify safe emails.

FILTER	DESCRIPTION	ENABLED BY DEFAULT
Whitelist	The Whitelist contains lists of criteria that identify legitimate email. Emails that match these criteria are not scanned by anti-spam filters and are always delivered to the recipient.	Yes
New Senders	The New Senders filter identifies emails that have been received from senders to whom emails have never been sent before.	No

2.5 Typical deployment scenarios

This chapter explains the different scenarios how GFI MailEssentials can be installed and configured.

2.5.1 Installing directly on Microsoft® Exchange server 21

2.5.2 Installing on an email gateway or relay/perimeter server 21

2.5.1 Installing directly on Microsoft® Exchange server

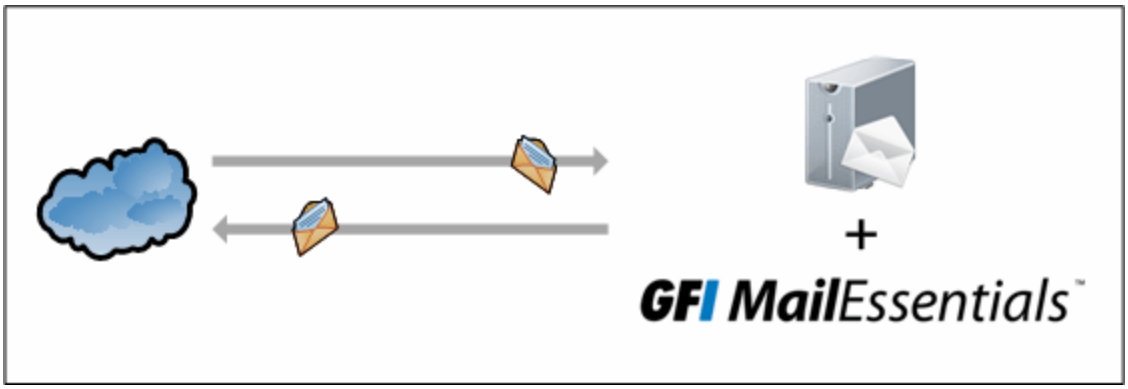


Figure 1: Installing GFI MailEssentials on your Microsoft® Exchange server

You can install GFI MailEssentials directly on Microsoft® Exchange Server 2003 or later, without any additional configuration.

NOTE

In Microsoft® Exchange 2007/2010 environments, GFI MailEssentials can only be installed on the servers with the following roles:

- Edge Server Role, or
- Hub Transport Role, or
- Hub Transport and Mailbox Roles - with this configuration GFI MailEssentials can also scan internal emails for viruses.

NOTE

GFI MailEssentials supports a number of mail servers but can only be installed on the same machine as Microsoft® Exchange. For other mail servers, for example Lotus Domino, install GFI MailEssentials on a separate machine.

2.5.2 Installing on an email gateway or relay/perimeter server

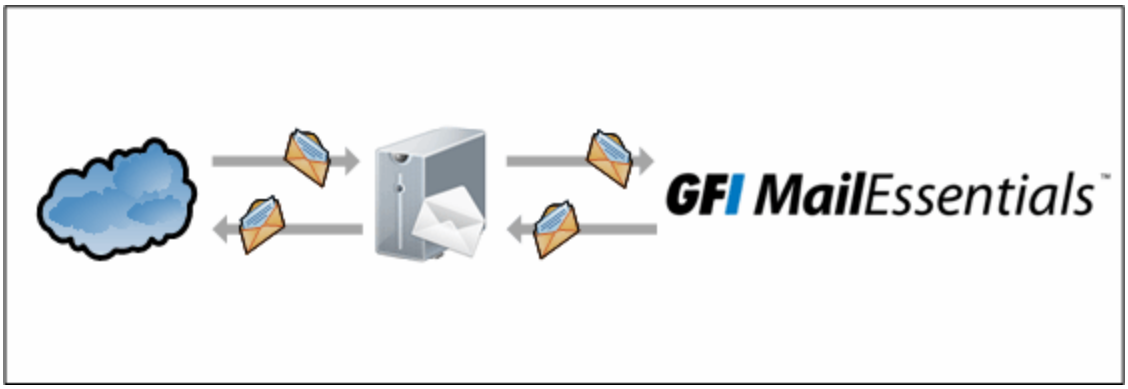


Figure 2: Installing GFI MailEssentials on a mail gateway/relay server

This setup is commonly used to filter spam on a separate machine, commonly installed in the DMZ. In this environment a server (also known as a gateway/perimeter server) is set to relay emails to the mail server. GFI MailEssentials is installed on the gateway/perimeter server so that spam and email malware is filtered before reaching the mail server.

This method enables you to filter out blocked emails before these are received on the mail server and reduce unnecessary email traffic. It also provides additional fault tolerance, where if the mail server is down, you can still receive email since emails are queued on the GFI MailEssentials machine.

When installing on a separate server (that is, on a server that is not the mail server), you must first configure that machine to act as a gateway (also known as “Smart host” or “Mail relay” server). This means that all inbound email must pass through GFI MailEssentials for scanning before being relayed to the mail server for distribution. For outbound emails, the mail server must relay all outgoing emails to the gateway machine for scanning before they are sent to destination.

If using a firewall, a good way to deploy GFI MailEssentials in the DMZ. GFI MailEssentials will act as a smart host/mail relay server when installed on the perimeter network (also known as DMZ - demilitarized zone).

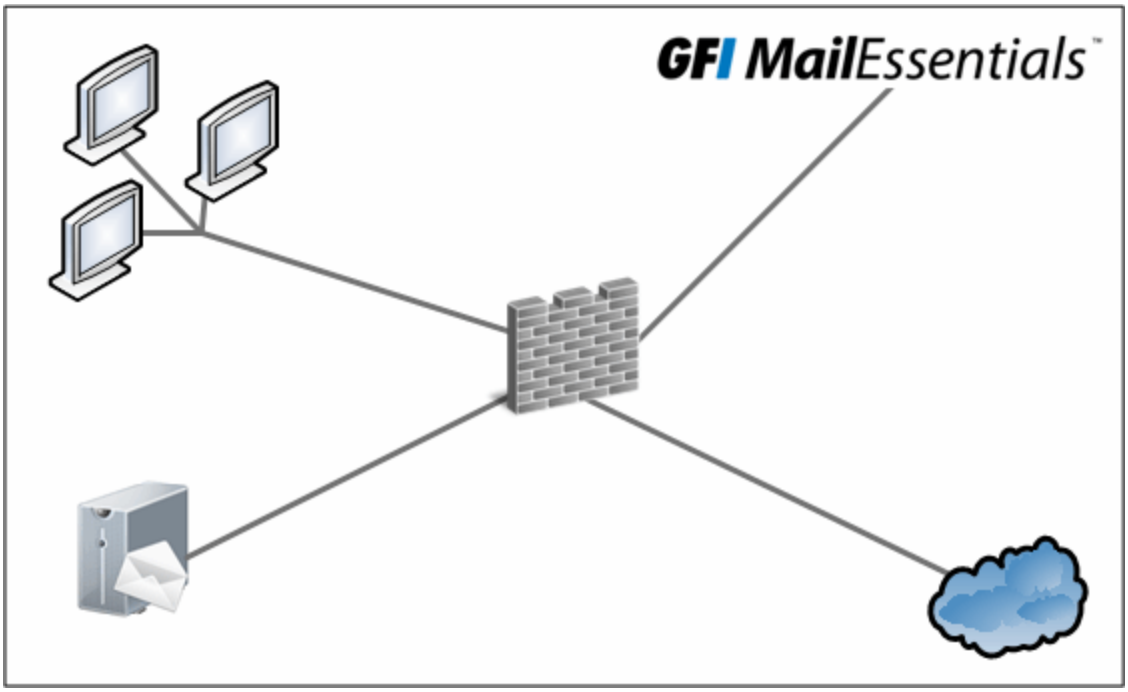


Figure 3: Installing GFI MailEssentials on a separate machine on a DMZ

NOTE

If GFI MailEssentials is installed on the perimeter server, you can use the anti-spam filters that run at SMTP level - Directory Harvesting and Greylist.

NOTE

In Microsoft® Exchange Server 2007/2010 environments, mail relay servers in a DMZ can be running Microsoft® Exchange Server 2007/2010 with the Edge Transport Server Role.

NOTE

Configure the IIS SMTP service to relay emails to your mail server and configure the MX record of your domain to point to the gateway machine. For more information, refer to Installing on an email gateway or relay/perimeter server (page 28).

3 Installation

The scope of this chapter is to help you install GFI MailEssentials on your network with minimum configuration effort.

Topics in this chapter:

3.1 System requirements 24
3.1.1 Hardware requirements 24
3.1.2 Processor 24
3.1.3 Available Memory (RAM) 24
3.1.4 Free Disk Space 24
3.1.5 Software requirements 25
3.1.6 Antivirus and backup software 26
3.1.7 Firewall port settings 27
3.2 Pre-installation actions 28
3.2.1 Installing on the Microsoft® Exchange server 28
3.2.2 Installing on an email gateway or relay/perimeter server 28
3.3 Installation procedure 32
3.3.1 Important notes 32
3.3.2 Running the installation wizard 33
3.3.3 Post-Installation Wizard 36
3.4 Upgrading a previous version 40
3.4.1 Upgrade Procedure 40
3.5 Post-Install actions 41
3.5.1 Add engines to the Windows DEP Exception List 42
3.5.2 Test your installation 43

3.1 System requirements

3.1.1 Hardware requirements

The minimum hardware requirements for GFI MailEssentials are:

3.1.2 Processor

- Minimum: 1Ghz
- Recommended: 2GHz with multiple cores

3.1.3 Available Memory (RAM)

- Minimum: 1.2GB
- Recommended: 1.5GB

3.1.4 Free Disk Space

- Minimum: 6GB
- Recommended: 10GB

NOTE

Hardware requirements depend on a range of factors including email volume, and number of Anti Virus engines enabled in GFI MailEssentials. The requirements specified above are required for GFI MailEssentials only.

3.1.5 Software requirements

Supported Operating Systems

- Windows® Server 2003 Standard or Enterprise (x86 or x64)(including R2) or later (including Microsoft® Windows Server 2012 - Standard and DataCenter editions).

Supported Mail Servers

GFI MailEssentials can be installed on the following mail servers without any further configuration.

- Microsoft® Exchange Server 2013

NOTE

Information Store Protection (VSAPI) is not supported on Microsoft® Exchange Server 2013 because VSAPI was removed from Microsoft® Exchange Server 2013 by Microsoft.

- Microsoft® Exchange Server 2010
- Microsoft® Exchange Server 2007 SP1 or higher
- Microsoft® Exchange Server 2003

For more information, refer to Installing on the Microsoft® Exchange server (page 28).

GFI MailEssentials can also be installed in an environment with any SMTP compliant mail server. In this case, GFI MailEssentials should be installed on the gateway/perimeter server so that spam is filtered before reaching the mail server.

For more information, refer to Installing on an email gateway or relay/perimeter server (page 28).

Supported Internet browsers

GFI MailEssentials can be used with the following Internet browsers:

- Microsoft Internet Explorer 8 or later
- Google Chrome version 22.0.1229.94 (October 10, 2012) or later.
- Mozilla Firefox version 16.0.2 (October 26, 2012) or later.

Other required components

- Internet Information Services (IIS®) World Wide Web service
- Internet Information Services (IIS®) SMTP service - Except when installing on Microsoft® Exchange 2007 /2010 server
- Microsoft.NET® Framework 4
- ASP.NET® 4.0

- Windows® Authentication role and Static Content services - Required when installing on Microsoft® Windows Server 2008/2008R2
- MSMQ - Microsoft® Messaging Queuing Service - for more information how to install MSMQ, refer to:

http://go.gfi.com/?pageid=ME_MSMQ

NOTE

For more information on how to install pre-requisites on Microsoft Windows® Server 2008 refer to:

http://go.gfi.com/?pageid=ME_Win2008

For more information on how to install pre-requisites on Microsoft Windows® Server 2012 refer to:

http://go.gfi.com/?pageid=ME_Win2012

NOTE

GFI MailEssentials Information Store Protection cannot be used if any other software is registered to make use of Microsoft® Exchange VSAPI.

NOTE

GFI MailEssentials can also be installed in virtual environments such as Microsoft® Hyper-V and VMWare virtualization software.

- Microsoft Virtual Server cluster group resource with a physical disc cluster. This is required ONLY for environments running Microsoft® Exchange 2003 clusters. For more information, refer to Appendix 3 - Microsoft® Exchange 2003 Clusters (page 278).

NOTE

For more information on how to create a Resource Group for an Exchange Virtual Server in a Windows Server Cluster, refer to: http://go.gfi.com/?pageid=ME_Clusterresourcegrouphowto.

3.1.6 Antivirus and backup software

Antivirus and backup software scanning may cause GFI MailEssentials to malfunction. This occurs when such software denies access to certain files required by GFI MailEssentials.

Disable third party antivirus and backup software from scanning the following folders:

32-bit installations (x86)	64-bit installations (x64)
<..\Program Files\Common Files\GFI>	<..\Program Files (x86)\Common Files\GFI>
<GFI MailEssentials installation path>\GFI\MailEssentials\	
<..\Inetpub\mailroot> - if installed on a gateway machine.	

32-bit installations (x86)	64-bit installations (x64)
<..*Program Files\Exchsrvr\Mailroot*> - if installed on the same machine as Microsoft® Exchange 2003	
<..*Program Files\Microsoft\Exchange Server\TransportRoles*> - if installed on the same machine as Microsoft® Exchange 2007	
<..*Program Files\Microsoft\Exchange Server\V14\TransportRoles*> - if installed on the same machine as Microsoft® Exchange 2010	
<..*Program Files\Microsoft\Exchange Server\V15\TransportRoles*> - if installed on the same machine as Microsoft® Exchange 2013	

3.1.7 Firewall port settings

Configure your firewall to allow the ports used by GFI MailEssentials.

Port	Description
53 - DNS	Used by the following anti-spam filters: » IP DNS Blocklist » SpamRazer » URI DNS Blocklist
20 & 21 - FTP	Used by GFI MailEssentials to connect to **ftp.gfi.com** and retrieve latest product version information.
80 - HTTP	Used by GFI MailEssentials to download product patches updates for: » SpamRazer » Anti-Phishing » Bayesian Analysis » Antivirus definition files » Trojan and executable scanner » Email Exploit engine GFI MailEssentials downloads from the following locations: » http://update.gfi.com » http://update.gfisoftware.com » http://support.gfi.com » *.mailshell.com » *.spamrazer.gfi.com **NOTE** GFI MailEssentials can also be configured to download updates through a proxy server. For more information, refer to Proxy settings (page 221).
8013, 8015, 8021 - Remoting	These ports are used for inter-process communication. No firewall configuration is required to allow connections to or from the remoting ports since all the GFI MailEssentials processes run on the same server. **NOTE** Ensure that no other applications (except GFI MailEssentials) are listening on these ports. If other applications are using this ports, these ports can be changed. For more information, refer to Remoting ports (page 254).

Port	Description
389/636 - LDAP/LDAPS	This port is used in these scenarios: » **Microsoft® Exchange environment** - Required if the server running GFI MailEssentials does not have access/cannot get list of users from Active Directory, for example, in a DMZ environment or other environments which do not use Active Directory. » **Lotus Domino mail server environment** - Required to get email addresses from Lotus Domino server. » **Other SMTP mail server environments** - Required to get email addresses from SMTP server.

3.2 Pre-installation actions

Before installing GFI MailEssentials, prepare your environment for deployment.

3.2.1 Installing on the Microsoft® Exchange server 28

3.2.2 Installing on an email gateway or relay/perimeter server 28

3.2.1 Installing on the Microsoft® Exchange server

When installing GFI MailEssentials on the same server as Microsoft® Exchange 2003 or later, no pre-install actions or configurations are required.

NOTE

In Microsoft® Exchange 2007/2010 environments, GFI MailEssentials can only be installed on the servers with the following roles:

» Edge Server Role, or

» Hub Transport Role, or

» Hub Transport and Mailbox Roles - with this configuration GFI MailEssentials can also scan internal emails for viruses.

3.2.2 Installing on an email gateway or relay/perimeter server

GFI MailEssentials can be installed:

» On a perimeter server (for example, in a DMZ)

» As a mail relay server between the perimeter (gateway) SMTP server and mail server.

This setup is commonly used to filter spam on a separate machine, commonly installed in the DMZ. In this environment a server (also known as a gateway/perimeter server) is set to relay emails to the mail server. GFI MailEssentials is installed on the gateway/perimeter server so that spam and email malware is filtered before reaching the mail server.

GFI MailEssentials uses the IIS SMTP service as its SMTP Server and therefore the IIS SMTP service must be configured to act as a mail relay server. To do this:

Step 1: Enable IIS SMTP Service

Step 2: Create SMTP domains for email relaying

Step 3: Enable email relaying to your Microsoft® Exchange server

Step 4: Secure your SMTP email-relay server

Step 5: Enable your mail server to route emails via gateway

Step 6: Update your domain MX record to point to mail relay server

Step 7: Test your new mail relay server

Step 1: Enable IIS SMTP Service

Windows Server 2003

1. Go to **Start > Control Panel > Add or Remove Programs > Add/Remove Windows Components**.
2. Select **Application Server** and click **Details**.
3. Select **Internet Information Services (IIS)** and click **Details**.
4. Select the **SMTP Service** option and click **OK**.
5. Click **Next** to finalize your configuration.

Windows Server 2008

1. Launch Windows Server Manager.
2. Navigate to the **Features** node and select **Add Features**.
3. From the **Add Features Wizard** select **SMTP Server**.

> **NOTE**
>
> The SMTP Server feature might require the installation of additional role services and features. Click **Add Required Role Services** to proceed with installation.

4. In the following screens click **Next** to configure any required role services and features, and click **Install** to start the installation.
5. Click **Close** to finalize configuration.

Step 2: Create SMTP domain(s) for email relaying

1. Go to **Start > Control Panel > Administrative Tools > Internet Information Services (IIS) Manager**.
2. In the left pane, expand the respective server node. Right click **Default SMTP Virtual Server** and select **Properties**.
4. Expand **Default SMTP Virtual Server** node.
5. Right click **Domains** and select **New > Domain**.
6. Select **Remote** and click **Next**.
7. Specify organization domain name (for example, test.mydomain.com) and click **Finish**.

Step 3: Enable email relaying to your Microsoft® Exchange server

1. Right click on the new domain and select **Properties**.
2. Select **Allow the Incoming Mail to be Relayed to this Domain**.

3. Select **Forward all mail to smart host** and specify the IP address of the server managing emails in this domain. IP address must be enclosed in square brackets, for example, `[123.123.123.123]`, to exclude them from all DNS lookup attempts.

4. Click **OK** to finalize your configuration.

Step 4: Secure your SMTP email-relay server

If unsecured, your mail relay server can be exploited and used as an open relay for spam. To prevent this, it is recommended that you specify which mail servers can route emails through this mail relay server (for example, allow only specific servers to use this email relaying setup). To achieve this:

1. Go to **Start > Control Panel > Administrative Tools > Internet Information Services (IIS) Manager**.

2. In the left pane, expand the respective server node. Right click on **Default SMTP Virtual Server** and select **Properties**.

3. From the **Access** tab, select **Relay**.

4. Select **Only the list below** and click **Add**.

5. Specify IP(s) of the internal mail server(s) that are allowed to route emails through your mail relay server. You can specify:

- Single computers - Authorize one specific machine to relay email through this server. Use the DNS Lookup button to lookup an IP address for a specific host.
- Group of computers - Authorize specific computer(s) to relay emails through this server.
- Domain - Allow all computers in a specific domain to relay emails through this server.

> **NOTE**
>
> The **Domain** option adds a processing overhead that can degrade SMTP service performance. This is due to the reverse DNS lookup processes triggered on all IP addresses (within that domain) that try to route emails through this relay server.

Step 5: Enable your mail server to route emails via GFI MailEssentials

Microsoft® Exchange Server 2003

Set up SMTP connectors that forward all emails to GFI MailEssentials.

1. Start **Exchange System Manager**.
2. Right-click **Connectors**, click **New > SMTP Connector** and specify a connector name.
3. Select **Forward all mail through this connector to the following smart host**, and specify the IP of your GFI MailEssentials relay server within square brackets, for example, `[123.123.1.123]`.
4. Click **Add** and select the GFI MailEssentials email relay server.
5. Click **OK**.
6. Go to **Address Space** tab.
7. Click **Add**, select **SMTP** and click **OK**.

8. Enter domain name and click **OK**
9. Select **Allow messages to be relayed to these domains.**
10. Click **OK.**

Lotus Notes

For more information on how to setup Lotus Domino routing, refer to Installation Guide(Domino).

SMTP/POP3 mail server

Configure your mail server to route all inbound and outbound email through GFI MailEssentials. In the configuration program of your mail server, use the option to relay all outbound email via another mail server (this option is usually called something similar to **Forward all messages to host**. Enter the computer name or IP of the machine running GFI MailEssentials. Save the new settings and restart your mail server.

Step 6: Update your domain MX record to point to mail relay server

Update the MX record of your domain to point to the IP of the new mail relay server. If your DNS server is managed by your ISP, ask your ISP to update the MX record for you.

> **NOTE**
>
> If the MX record is not updated, all emails will be routed directly to your email server - hence bypassing GFI MailEssentials.

Verify that MX record has been successfully updated

To verify whether MX record is updated:

1. From command prompt key in `nslookup` and hit **Enter**.
2. Key in `set type=mx` and hit **Enter**.
3. Specify your mail domain name and hit **Enter**.

The MX record should return the IP addresses of the mail relay servers.

Step 7: Test your new mail relay server

Before proceeding to install GFI MailEssentials, verify that your new mail relay server is working correctly.

Test IIS SMTP inbound connection

1. Send an email from an 'external' account (example, from a Gmail account) to an internal email address/user.
2. Ensure that intended recipient received the test email in the respective email client.

Test IIS SMTP outbound connection

1. Send an email from an 'internal' email account to an external account (example, to a Gmail account).
2. Ensure that the intended recipient/external user received the test email.

NOTE

You can also use Telnet to manually send the test email and obtain more troubleshooting information. For more information refer to:

http://go.gfi.com/?pageid=ME_TelnetPort25

3.3 Installation procedure

This section describes how to run the installation of GFI MailEssentials.

3.3.1 Important notes

1. If you are currently using a previous version of GFI MailEssentials, you can upgrade your current installation while at the same time retaining all your existing configuration settings. For more information, refer to Upgrading a previous version (page 40).

IMPORTANT

Upgrade is not reversible; you cannot downgrade to the previous version you had installed.

IMPORTANT

For information on how to upgrade to GFI MailEssentials from VIPRE Email Security for Exchange refer to http://go.gfi.com/?pageid=ME_VPXUpgrade

2. If you are currently on SMA and you want to upgrade, access the GFI website customer area to upgrade your current license key.

NOTE

'Evaluation' is no longer accepted as a license key. Access the GFI website customer area to upgrade your license key before starting the upgrade process.

3. Download the appropriate GFI MailEssentials build for your type of machine. Use GFI MailEssentials 32-bit (x86) setup for 32-bit systems and the 64-bit (x64) setup for 64-bit systems.
4. Before running installation wizard, ensure that:

- You are logged on using an account with administrative privileges.
- The machine where GFI MailEssentials is going to be installed, meets the specified system requirements. For more information, refer to System requirements (page 24).
- Configure your firewall to allow GFI MailEssentials to connect to GFI servers. For more information, refer to Firewall port settings (page 27).
- Disable third-party antivirus and backup software from scanning folders used by GFI MailEssentials. For more information, refer to Antivirus and backup software (page 26).

- If installing GFI MailEssentials on an email gateway or relay/perimeter server, configure that machine to act as a gateway. For more information, refer to Installing on an email gateway or relay/perimeter server (page 28).
- Save any pending work and close all open applications on the machine.

5. GFI MailEssentials installation restarts Microsoft® Exchange or Microsoft IIS® SMTP services. This is required to allow GFI MailEssentials components to register correctly.

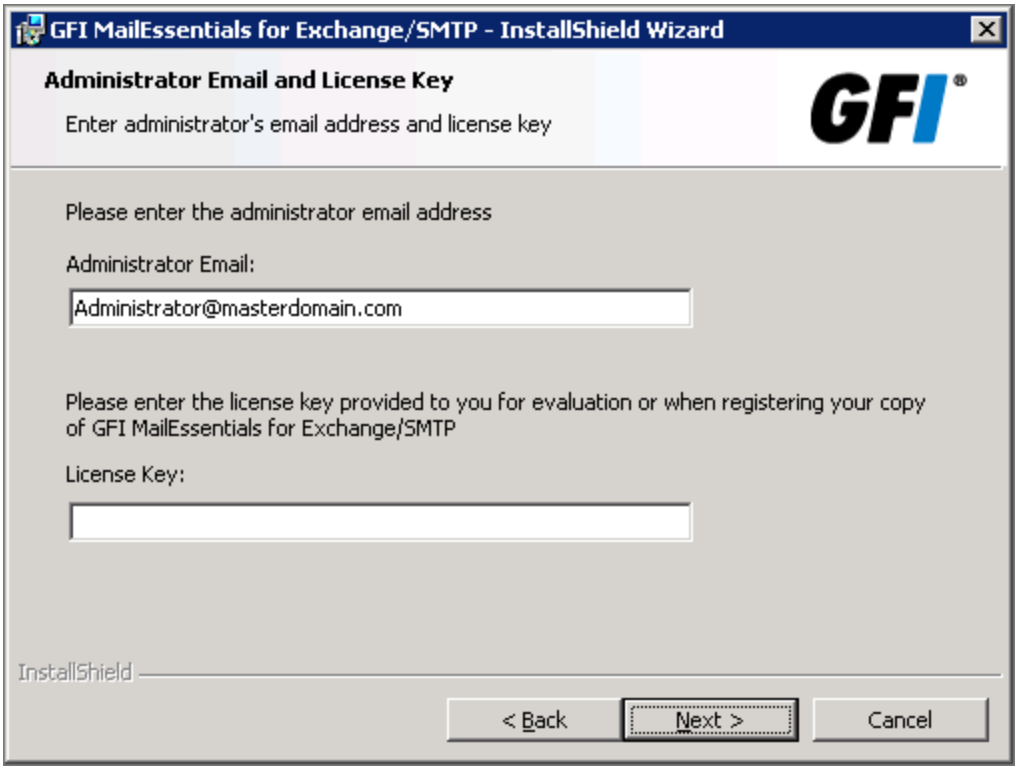
> **NOTE**
>
> It is recommended to install GFI MailEssentials at a time when restarting these services has the least impact on your network.

3.3.2 Running the installation wizard

1. Run the GFI MailEssentials setup program.
2. Select the language to use with this installation of GFI MailEssentials and click **Install**.

> **NOTE**
>
> Language selection is not reversible. You will need to reinstall GFI MailEssentials to change the language selected at this stage.

3. Click **Next** in the **Welcome** page.
4. Select whether to check for newer versions/builds of GFI MailEssentials and click **Next**.
5. Read the license agreement and click **I accept the terms in the license agreement** if you accept the terms and conditions. Click **Next**.


GFI MailEssentials for Exchange/SMTP - InstallShield Wizard
Administrator Email and License Key
Enter administrator's email address and license key
GFI
Please enter the administrator email address
Administrator Email:
Administrator@masterdomain.com
Please enter the license key provided to you for evaluation or when registering your copy of GFI MailEssentials for Exchange/SMTP
License Key:
InstallShield
< Back
Next >
Cancel

Screenshot 1: Specifying administrator's email address and license key

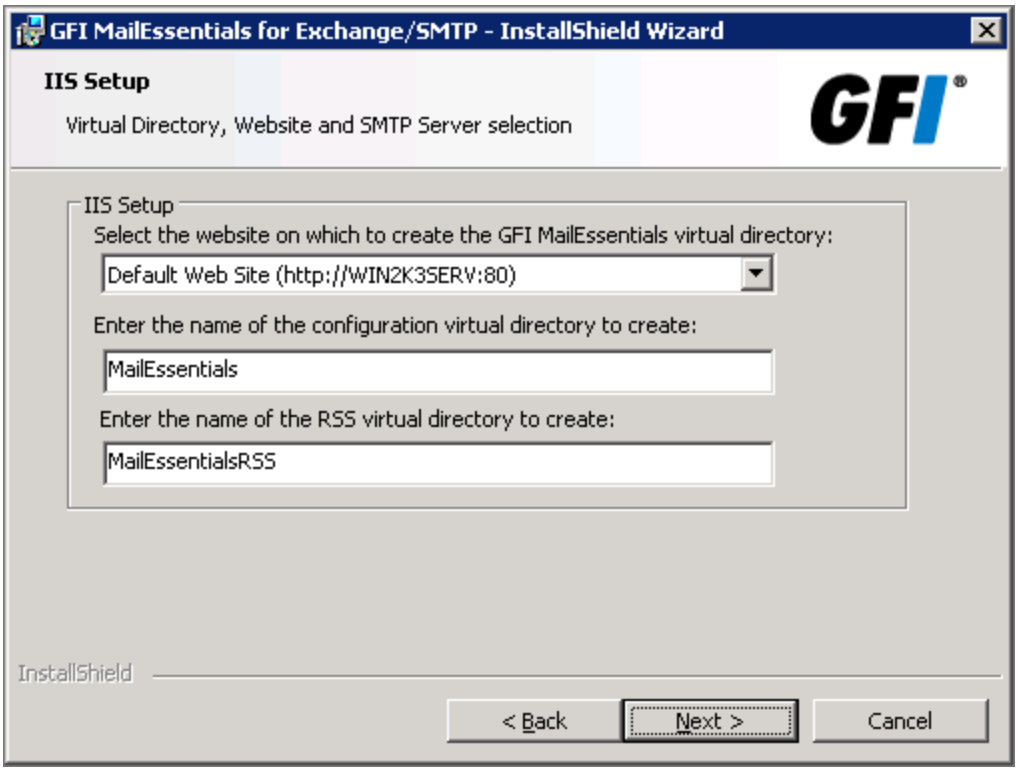
6. Key in the administrator's email address in the **Administrator Email** and enter **License Key**. Click **Next**.

> **NOTE**
>
> 'Evaluation' is no longer accepted as a license key. Access the GFI website customer area to upgrade your license key before starting the upgrade process.

7. Select the mode that GFI MailEssentials will use to retrieve the list of email users.

Option	Description
Yes, all email users are available on Active Directory. Rules will be based on Active Directory users.	**Active Directory mode** GFI MailEssentials will retrieve the list of users from Active Directory. Selecting this option means that GFI MailEssentials is being installed behind your firewall and that it has access to the Active Directory containing ALL your email users.
No, I do not have Active Directory or my network does not have access to Active Directory (DMZ)	**SMTP mode** Select this mode if you are installing GFI MailEssentials on a machine that does not have access to the Active Directory containing the complete list of all your email users. This includes machines on a DMZ or machines that are not part of the Active Directory domain. In this mode, GFI MailEssentials automatically populates the list of local users using the sender's email address in outbound emails. The list of users can also be managed from the GFI MailEssentials General Settings node. For more information, refer to Managing local users (page 222).

Click **Next**.


GFI MailEssentials for Exchange/SMTP - InstallShield Wizard
IIS Setup
Virtual Directory, Website and SMTP Server selection
GFI
IIS Setup
Select the website on which to create the GFI MailEssentials virtual directory:
Default Web Site (http://WIN2K3SERV:80)
Enter the name of the configuration virtual directory to create:
MailEssentials
Enter the name of the RSS virtual directory to create:
MailEssentialsRSS
InstallShield
< Back
Next >
Cancel

Screenshot 2: SMTP server and virtual directory details

8. In the **IIS Setup** dialog, configure the following options:

NOTE

Default settings are typically correct for most installations.

Option	Description
The website to create the GFI MailEssentials virtual directory	Select the website where you want to host the GFI MailEssentials virtual directories.
The GFI MailEssentials Configuration virtual directory	Specify a name for the GFI MailEssentials virtual directory.
The GFI MailEssentials Quarantine RSS feeds virtual directory	Specify a name for the GFI MailEssentials Quarantine RSS feeds virtual directory.
SMTP Server Setup	Select the SMTP Server that GFI MailEssentials binds to. By default, GFI MailEssentials binds to your Default SMTP Virtual Server. If you have multiple SMTP virtual servers on your domain, you can bind GFI MailEssentials to any available SMTP virtual server. **NOTES** 1. If you are installing on a Microsoft® Exchange Server 2007/2010/2013 machine this option is not shown since Microsoft® Exchange has its own built-in SMTP server. 2. After installation, you can still bind GFI MailEssentials to another SMTP virtual server from the GFI MailEssentials Configuration. For more information, refer to SMTP Virtual Server bindings (page 223).

Click **Next**.

9. Select folder where to install GFI MailEssentials and click **Next**.

NOTE

When the installation is an upgrade, GFI MailEssentials installs in the same location as the previous installation.

10. Click **Install** to start the installation process.

NOTE

If you are prompted to restart the SMTP services, click **Yes**.

11. On completion, click **Finish**.

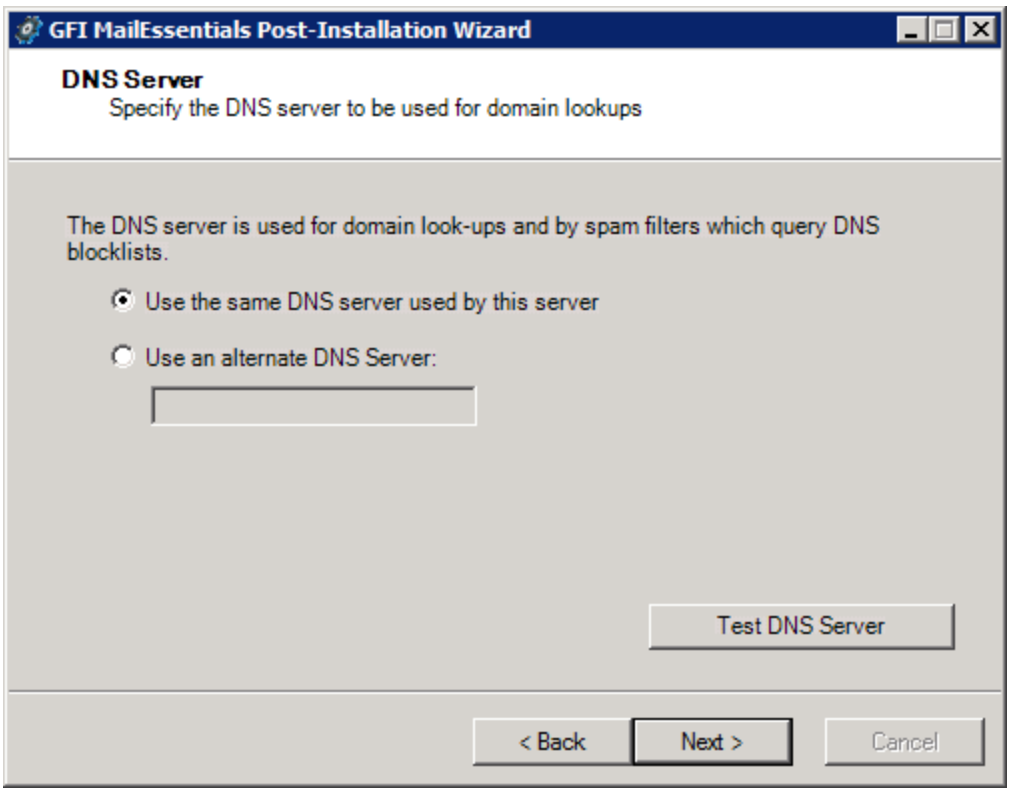
NOTE

For new installations, setup will launch the Post-Installation Wizard. For more information, refer to Post-Installation Wizard (page 36).

3.3.3 Post-Installation Wizard

The post-installation wizard loads automatically after installing GFI MailEssentials the first time. It enables configuration of the most important settings of GFI MailEssentials.

1. Click **Next** in the welcome page.

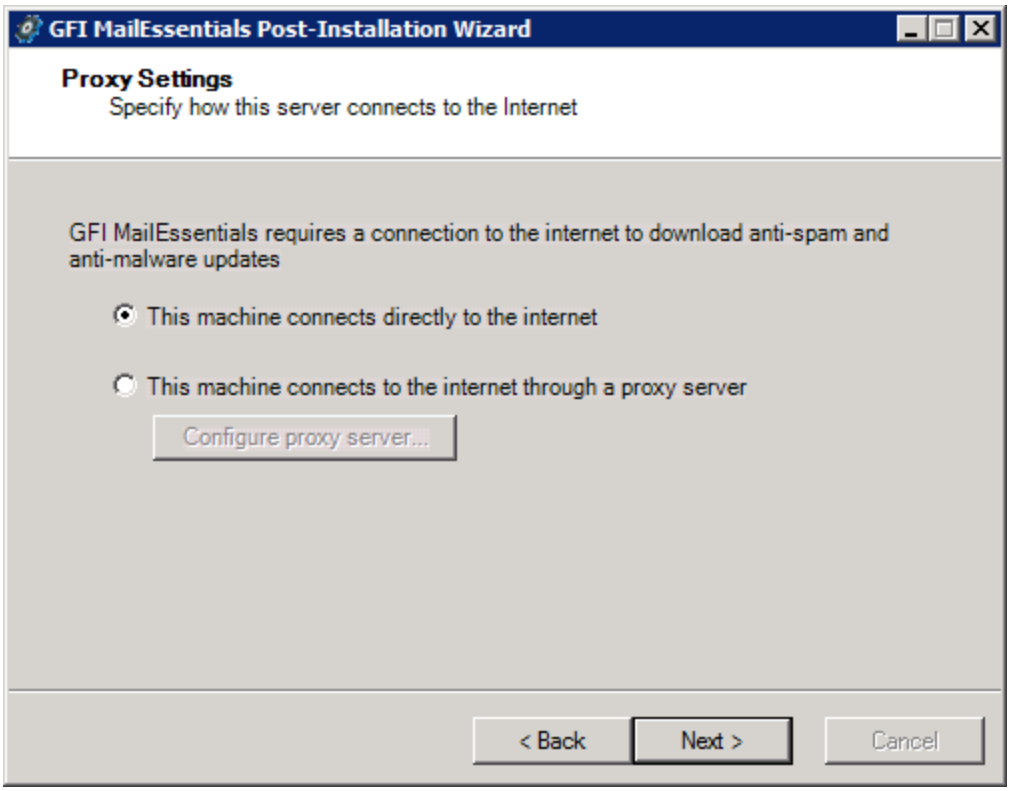

GFI MailEssentials Post-Installation Wizard
DNS Server
Specify the DNS server to be used for domain lookups
The DNS server is used for domain look-ups and by spam filters which query DNS blocklists.
Use the same DNS server used by this server
Use an alternate DNS Server:
Test DNS Server
< Back
Next >
Cancel

Screenshot 3: DNS Server settings

2. In the DNS Server dialog, select:

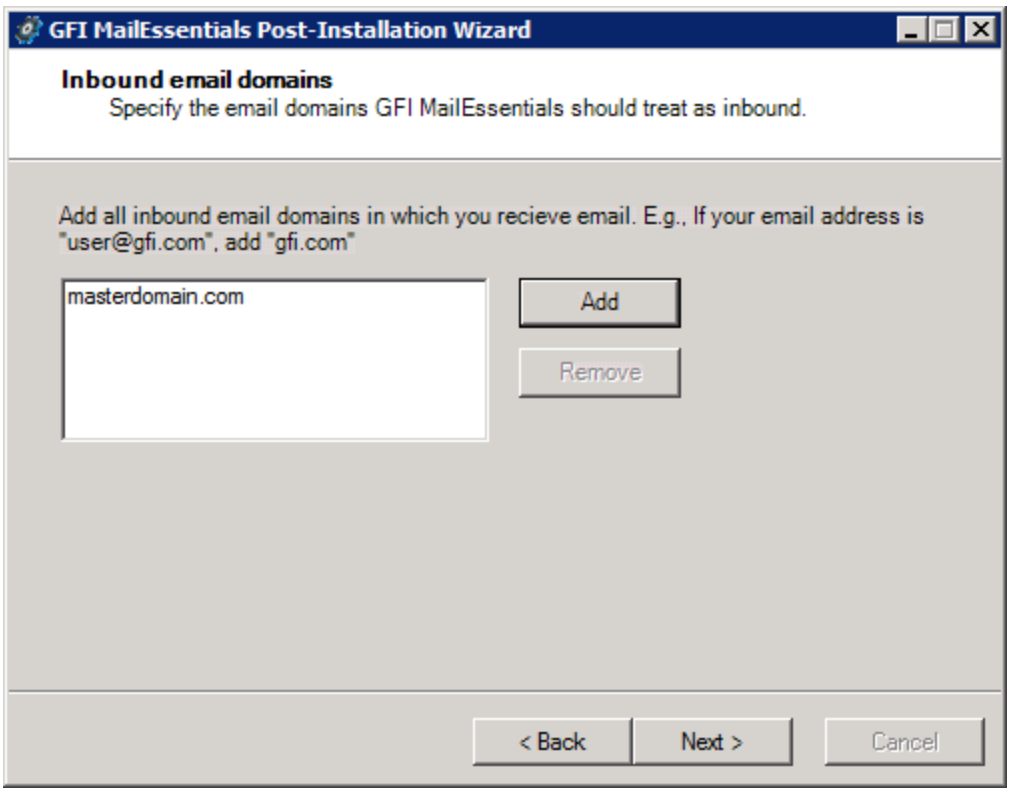
Option	Description
Use the same DNS server used by this server	Select this option to use the same DNS server that is used by the operating system where GFI MailEssentials is installed.
Use an alternate DNS server	Select this option to specify a custom DNS server IP address.

Click **Test DNS Server** to test connection with the specified DNS server. If test is unsuccessful, specify another DNS server. Click **Next**.


GFI MailEssentials Post-Installation Wizard
Proxy Settings
Specify how this server connects to the Internet
GFI MailEssentials requires a connection to the internet to download anti-spam and anti-malware updates
This machine connects directly to the internet
This machine connects to the internet through a proxy server
Configure proxy server...
< Back
Next >
Cancel

Screenshot 4: Proxy settings

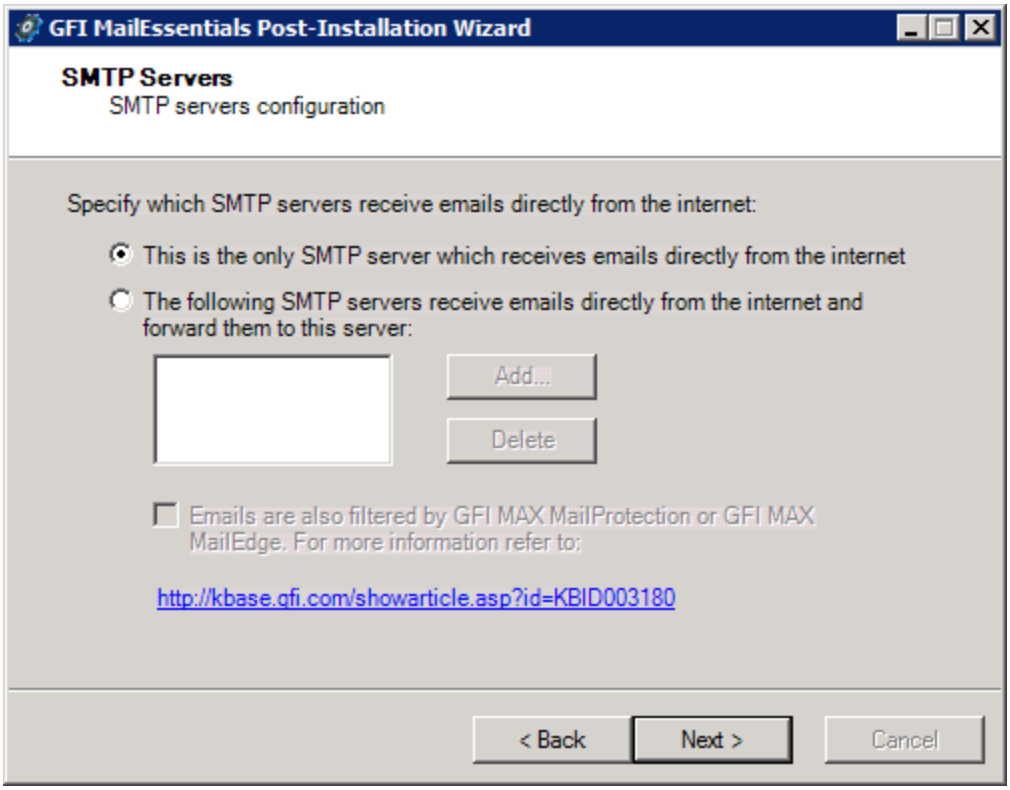
3. In the **Proxy Settings** dialog, specify how GFI MailEssentials connects to the Internet. If the server connects through a proxy server click **Configure proxy server…** and specify proxy settings. Click **Next**.


GFI MailEssentials Post-Installation Wizard
Inbound email domains
Specify the email domains GFI MailEssentials should treat as inbound.
Add all inbound email domains in which you recieve email. E.g., If your email address is "user@gfi.com", add "gfi.com"
masterdomain.com
Add
Remove
< Back
Next >
Cancel

Screenshot 5: Inbound email domains

4. In the **Inbound email domains** dialog specify all the domains to scan for viruses and spam. Any local domains that are not specified in this list will not be scanned. Click **Next**.

> **NOTE**
>
> When adding domains, select **Obtain domain's MX records and include in perimeter servers list** to retrieve the domain's MX records and automatically add them to the perimeter SMTP servers list (configured in the next step).

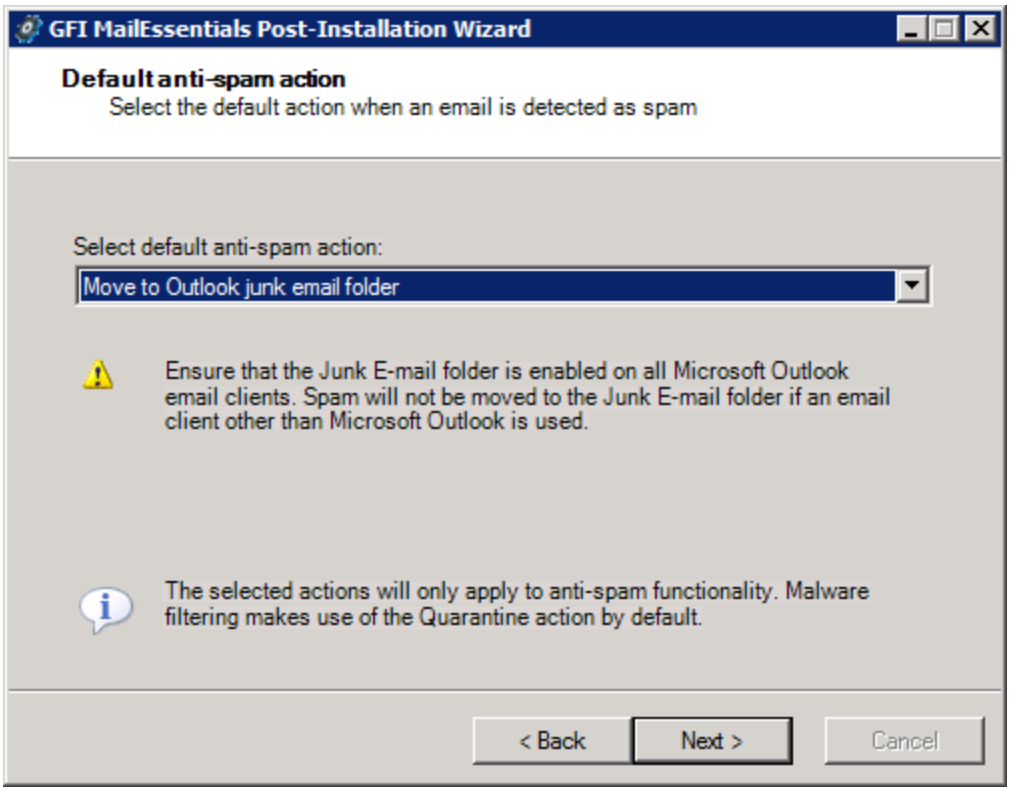

GFI MailEssentials Post-Installation Wizard
SMTP Servers
SMTP servers configuration
Specify which SMTP servers receive emails directly from the internet:
This is the only SMTP server which receives emails directly from the internet
The following SMTP servers receive emails directly from the internet and forward them to this server:
Add...
Delete
Emails are also filtered by GFI MAX MailProtection or GFI MAX MailEdge. For more information refer to:
http://kbase.gfi.com/showarticle.asp?id=KBID003180
< Back
Next >
Cancel

Screenshot 6: SMTP Server settings

5. In the **SMTP Servers** dialog specify how the server receives external emails. If emails are routed through other servers before they are forwarded to GFI MailEssentials, add the IP address of the other servers in the list. For more information about perimeter SMTP servers refer to: http://go.gfi.com/?pageid=ME_PerimeterServer

   When using hosted email security products GFI MAX MailProtection, GFI MAX MailEdge or GFI MailEssentials Online, enable checkbox **Emails are also filtered by…**. For more information refer to: http://go.gfi.com/?pageid=ME_MAXMPME.

Click **Next**.


GFI MailEssentials Post-Installation Wizard
Default anti-spam action
Select the default action when an email is detected as spam
Select default anti-spam action:
Move to Outlook junk email folder
Ensure that the Junk E-mail folder is enabled on all Microsoft Outlook email clients. Spam will not be moved to the Junk E-mail folder if an email client other than Microsoft Outlook is used.
The selected actions will only apply to anti-spam functionality. Malware filtering makes use of the Quarantine action by default.
< Back
Next >
Cancel

Screenshot 7: Selecting the default anti-spam action to use

6. In the **Default anti-spam action** dialog select the default action to be taken when emails are detected as spam.

> **NOTE**
>
> This action applies to anti-spam filters only. Malware filters automatically quarantine blocked emails. For more information, refer to Email scanning and filtering engines (page 19).

> **NOTE**
>
> When installing on Microsoft® Exchange 2010 and the default action selected is **Move to mailbox sub-folder**, a user with impersonation rights must be created. Select whether to let GFI MailEssentials automatically create the user or manually specify the credentials and click **Set impersonation rights** to assign the required rights to the specified user. This user must be dedicated to this feature only and the credentials must not be changed. For more information refer to http://go.gfi.com/?pageid=ME_SpamExch2010.

Click **Next**.

7. When installing on Microsoft® Exchange Server 2007/2010, the list of Microsoft® Exchange server roles detected and GFI MailEssentials components required is displayed. Click **Next** to install the required GFI MailEssentials components.
8. Click **Finish** to finalize the installation.

GFI MailEssentials installation is now complete and the email protection system is up and running.

Next step: Optimize your protection system to ensure that it is effectively up and running. For more information, refer to Post-Install actions (page 41).

NOTE

To re-run the Post-Installation wizard, from command prompt, navigate to the GFI MailEssentials installation folder and run the following command:

```
e2kwiz.exe clean
```

3.4 Upgrading a previous version

GFI MailEssentials enables you to upgrade existing installations of GFI MailEssentials and/or GFI MailSecurity. The following restrictions on versions apply:

Product	Restriction
GFI MailEssentials	Minimum version to upgrade from: GFI MailEssentials 12 with all Service Releases installed.
GFI MailSecurity	Minimum version to upgrade from: GFI MailSecurity 10.1 with all Service Releases installed.

If upgrading an installation with a previous version of GFI MailEssentials, GFI MailEssentials is installed with Anti-Spam and Anti-Phishing features fully licensed and the Anti-Virus and Anti-Malware on a 30 day trial period. Likewise, if upgrading an installation where only GFI MailSecurity is installed, only the Anti-Virus and Anti-Malware features are fully licensed, while the Anti-Spam and Anti-Phishing features are on a 30 day trial period. Installations where both GFI MailEssentials and GFI MailSecurity are installed are upgraded to have both Anti-Spam/Anti-Phishing and Anti-Virus/Anti-Malware features fully licensed.

For more information on GFI MailEssentials licensing, refer to http://go.gfi.com/?pageid=ME_adminManualEN

IMPORTANT

Before upgrading to the latest version of GFI MailEssentials, ensure your system meets the minimum system requirements. For more information, refer to System requirements (page 24).

3.4.1 Upgrade Procedure

IMPORTANT

Upgrade is not reversible; you cannot downgrade to the previous version you had installed.

Select the configuration option that best describes your setup from the list below.

- Previous installation on SMTP Server/Microsoft Exchange Server 2003
- Previous installation on Microsoft Exchange Server 2007/2010
- Updating to a newer version of GFI MailEssentials

Previous installation on SMTP Server/Microsoft® Exchange Server 2003

Only previous version of GFI MailSecurity is installed

Install GFI MailEssentials as if installing for the first time. For more information, refer to Installation procedure (page 32). Following the installation, also complete the GFI MailEssentials Post Install Wizard. For more information, refer to Post-Installation Wizard (page 36).

Only previous version of GFI MailEssentials is installed

Install GFI MailEssentials as if installing for the first time. For more information, refer to Installation procedure (page 32).

Both previous versions of GFI MailEssentials and GFI MailSecurity are installed

Install GFI MailEssentials as if installing for the first time. For more information, refer to Installation procedure (page 32).

Previous installation on Microsoft® Exchange Server 2007/2010

Only previous version of GFI MailSecurity is installed

Install GFI MailEssentials as if installing for the first time. For more information, refer to Installation procedure (page 32). Following the installation, also complete the GFI MailEssentials Post Install Wizard. For more information, refer to Post-Installation Wizard (page 36).

Only previous version of GFI MailEssentials is installed

Install GFI MailEssentials as if installing for the first time. For more information, refer to Installation procedure (page 32).

Both previous versions of GFI MailEssentials and GFI MailSecurity are installed

Install GFI MailEssentials as if installing for the first time. For more information, refer to Installation procedure (page 32).

Updating to a newer versions of GFI MailEssentials

The GFI MailEssentials installer also enables you to upgrade an existing version of the current generation of GFI MailEssentials to a newer version; for example, from a Beta version to Release version.

To upgrade, launch the latest installer on the server where GFI MailEssentials is installed. After accepting the End User License Agreement, installer detects existing installation and shows the previous version installation path. Click **Next** to upgrade and **Finish** on completion.

NOTE

For upgrades on Microsoft® Exchange 2007/2010 the Post Installation wizard is displayed after the installation and only displays the list of Microsoft® Exchange server roles detected and the GFI MailEssentials components required. Click **Next** to install the required GFI MailEssentials components and **Finish** to complete Post-Install wizard.

3.5 Post-Install actions

To ensure GFI MailEssentials scanning and filtering system is effectively up and running, perform the following post-install actions:

Action	Description
Add GFI MailEssentials scanning engines to the Windows DEP Exception List.	Data Execution Prevention (DEP) is a set of hardware and software technologies that perform memory checks to help prevent malicious code from running on a system. If you installed GFI MailEssentials on an operating system that includes DEP, you will need to add the GFI MailEssentials scanning engine (**GFiScanM.exe**) and the Kaspersky Virus Scanning Engine (**kavss.exe**) executables. **NOTE** This is required only when installing on Microsoft® Windows Server 2003 SP 1 or SP 2. For more information, refer to Add engines to the Windows DEP Exception List (page 42).
Launch GFI MailEssentials Configuration	Go to **Start > Programs > GFI MailEssentials > GFI MailEssentials Configuration.**
Enable Directory Harvesting	Directory harvesting attacks occur when spammers try to guess email addresses by attaching well known usernames to your domain. The majority of the email addresses are non-existent. This filter is enabled by default if GFI MailEssentials is installed in an Active Directory Environment. For more information, refer to Directory Harvesting (page 107).
Enable Greylist	The Greylist filter temporarily blocks incoming emails received from unknown senders. Legitimate mail systems typically try to send the email after a few minutes; spammers simply ignore such error messages. This filter is not enabled by default. For more information, refer to Greylist (page 119).For more information, refer to Greylist (page 119).
Configure Whitelists	The Whitelist contains lists of criteria that identify legitimate email. Emails that match these criteria are not scanned by anti-spam filters and are always delivered to the recipient. For more information, refer to Whitelist (page 130).
Test your installation	After configuring all post-install actions, GFI MailEssentials is ready to start protecting and filtering your mail system from malicious and spam emails. Test your installation to ensure that GFI MailEssentials is working properly. For more information, refer to Test your installation (page 43).

3.5.1 Add engines to the Windows DEP Exception List

Data Execution Prevention (DEP) is a set of hardware and software technologies that perform memory checks to help prevent malicious code from running on a system.

If you installed GFI MailEssentials on an operating system that includes DEP, you will need to add the GFI MailEssentials scanning engine (**GFiScanM.exe**) and the Kaspersky Virus Scanning Engine (**kavss.exe**) executables.

NOTE

This is required only when installing on Microsoft® Windows Server 2003 SP 1 or SP 2.

To add the GFI executables in the DEP exception list:

1. From **Control Panel** open the **System** applet.
2. From the **Advanced** tab, under the **Performance** area, click **Settings**.
3. Click **Data Execution Prevention** tab.
4. Click **Turn on DEP for all programs and services except those I select**.
5. Click **Add** and from the dialog box browse to: ***<GFI MailEssentials installation path>**GFI**MailEssentials*\EmailSecurity**, and choose **GFiScanM.exe**.

6. Click **Add** and from the dialog box browse to: **<*GFI MailEssentials installation path*>*GFI**MailEssentials*\AntiVirus\Kaspersky**, and choose **kavss.exe**.

7. Click **Apply** and **OK** to apply the changes.

8. Restart the **GFI MailEssentials Autoupdater** service and the **GFI MailEssentials AV Scan Engine** services.

3.5.2 Test your installation

After configuring all post-install actions, GFI MailEssentials is ready to start protecting and filtering your mail system from malicious and spam emails.

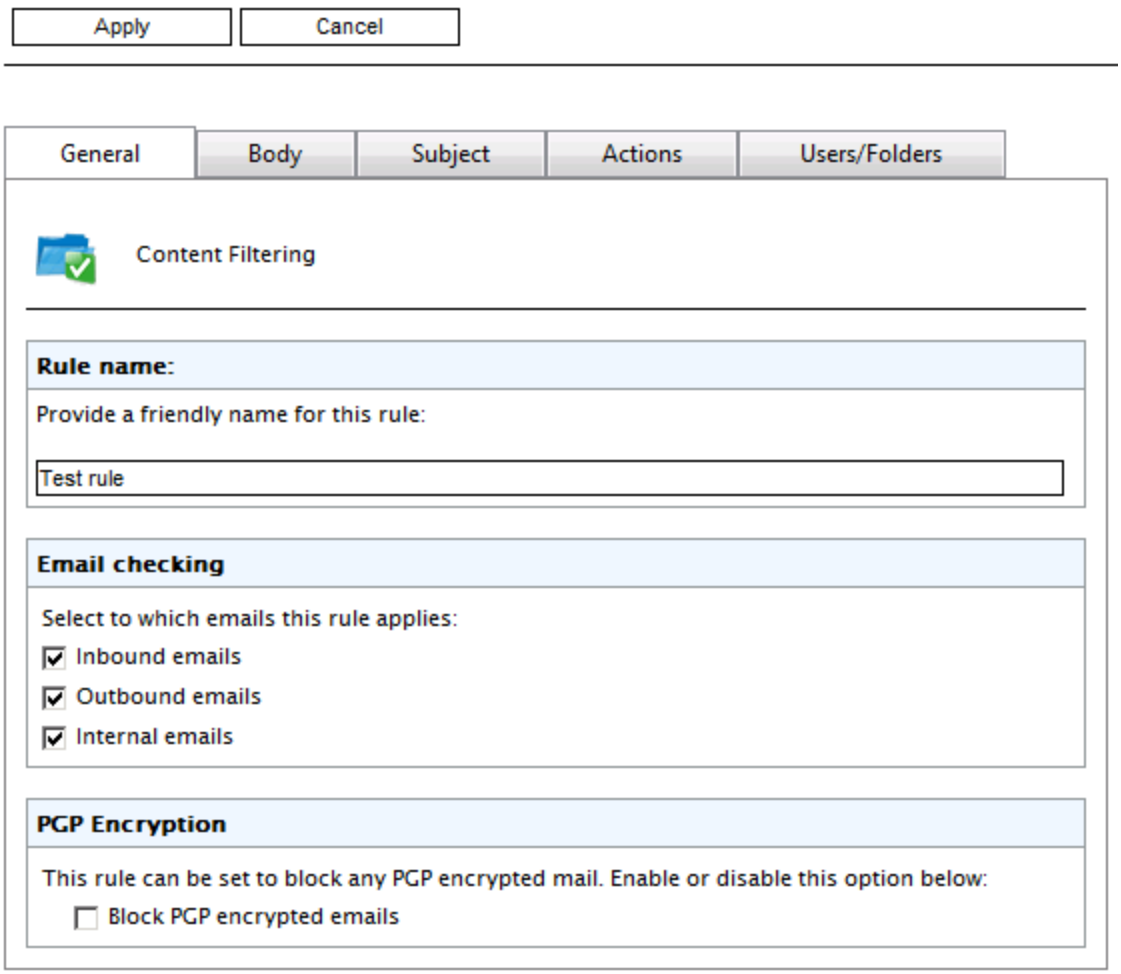
Ensure that GFI MailEssentials blocks unwanted emails. To do this, send inbound and outbound test emails that are purposely composed in such a way that they are blocked by GFI MailEssentials.

Step 1: Create a Content Filtering rule

1. Launch the GFI MailEssentials console.

2. Go to **GFI MailEssentials > Content Filtering > Keyword Filtering** node.

3. Click **Add Rule…**.



Screenshot 8: Creating a test rule on Keyword filtering

4. In **Rule name** type `Test Rule`.

5. From the **Subject** tab, select **Block emails if content is found matching these conditions (message subject)**.

6. In **Edit Condition** type `Threat test` and click **Add Condition**.

7. From **Actions** tab, enable **Block email and perform this action** and select **Quarantine email**.

8. Click **Apply** to save the rule.

Step 2: Send an inbound test email

1. From an external email account, create a new email and type `Threat test` as the subject.

2. Send the email to one of your internal email accounts.

Step 3: Send an outbound test email

1. From an internal email account, create a new email and type `Threat test` as the subject.

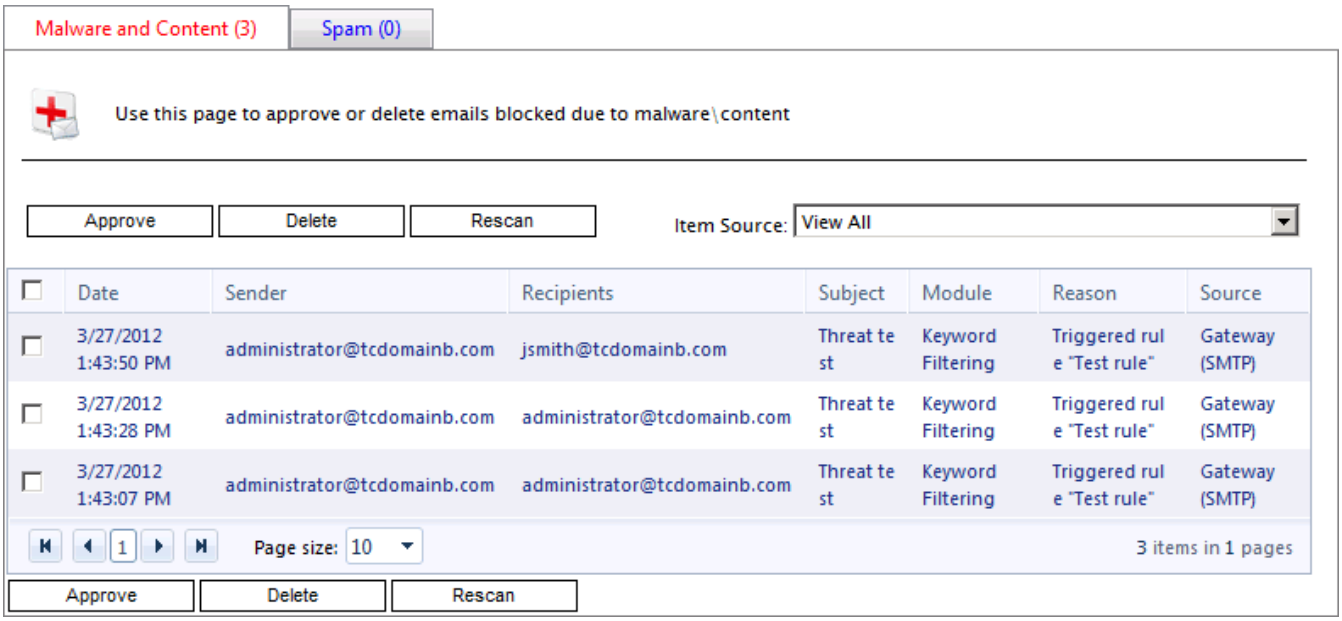
2. Send the email to an external email account.

Step 4: Confirm that test emails are blocked

Verify that both inbound and outbound test emails are blocked and quarantined. To do this:

1. From GFI MailEssentials, go to **GFI MailEssentials Configuration > Quarantine > Today**.

2. Ensure that both inbound and outbound test emails are listed in **Malware and Content** tab, reason being: **Triggered rule "Test rule"**.



Screenshot 9: Test email blocked by Test rule

NOTE

When test is completed successfully, delete or disable **Test rule** created in step 1.

4 Monitoring status

GFI MailEssentials enables monitoring of your email activity in real time or by generating reports of email activity for a particular time period.

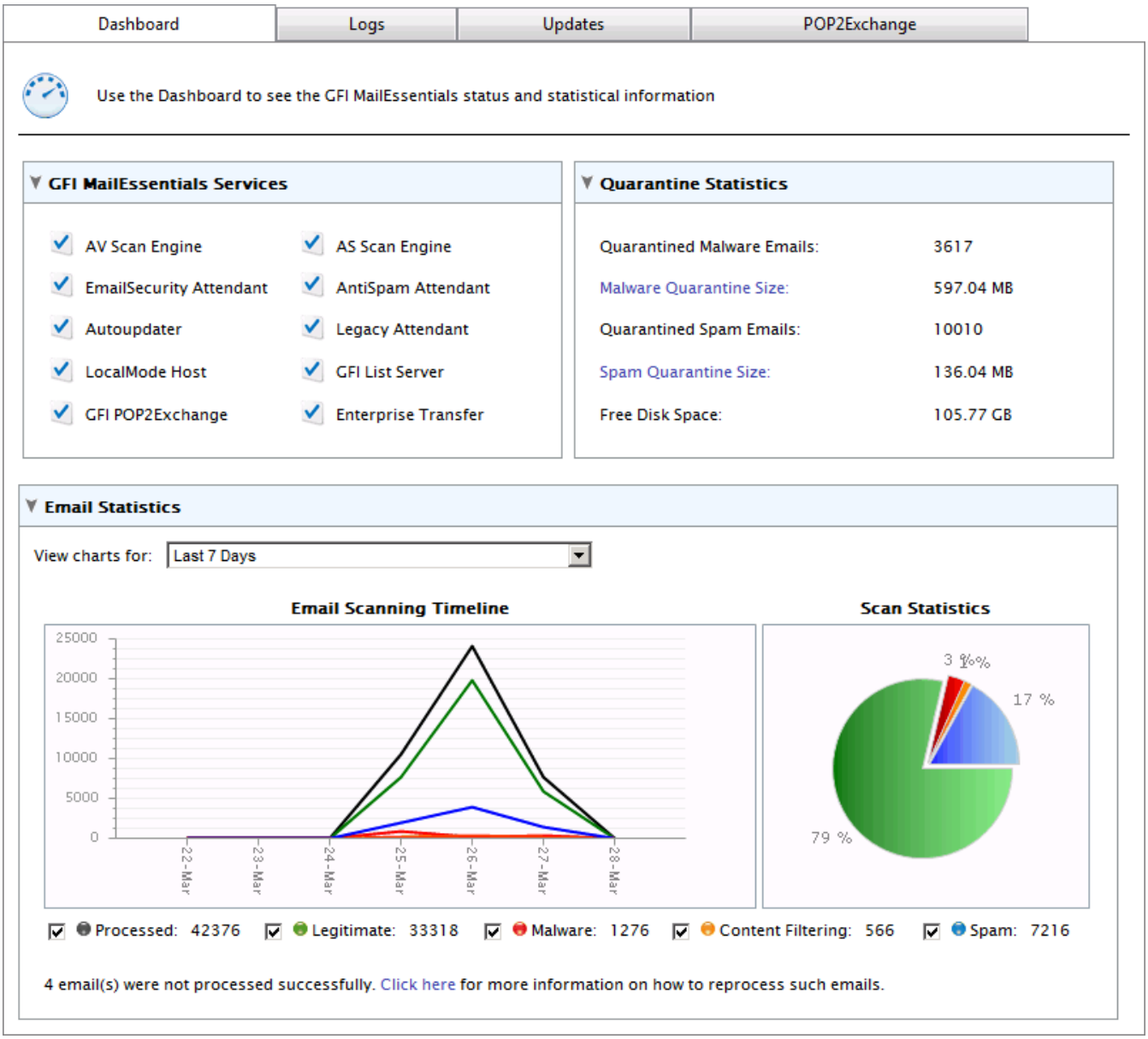
Monitoring module	Description
Dashboard	The GFI MailEssentials **Dashboard** provides real time information that enables you to monitor the product. To access the Dashboard, go to **GFI MailEssentials > Dashboard**. This includes: » Important statistical information about blocked emails. For more information, refer to Status and statistics (page 46). » Status of GFI MailEssentials services. For more information, refer to Services (page 47). » Graphical presentation of email activity. For more information, refer to Charts (page 48). » List of emails processed. For more information, refer to Email processing logs (page 49). » Status of software updates. For more information, refer to Antivirus and anti-spam engine updates (page 51). » Log of POP2Exchange activities. For more information, refer to POP2Exchange activity (page 52).
Reports	GFI MailEssentials enables you to create reports based on data logged to database. To access Reporting, go to **GFI MailEssentials > Reporting**. » **Enabling reporting** - For more information, refer to Enabling/Disabling reporting (page 52). » **Configure reporting database** - For more information, refer to Configuring reporting database (page 58). » **Generate reports** - For more information, refer to Generating a report (page 53). » **Create custom reports** - For more information, refer to Custom reports (page 56). » **Search the reporting database** - For more information, refer to Searching the reporting database (page 57).

4.1 Dashboard

The GFI MailEssentials **Dashboard** provides real time information that enables you to monitor the product. To access the Dashboard, go to **GFI MailEssentials > Dashboard**. This includes:

- Important statistical information about blocked emails. For more information, refer to Status and statistics (page 46).
- Status of GFI MailEssentials services. For more information, refer to Services (page 47).
- Graphical presentation of email activity. For more information, refer to Charts (page 48).
- List of emails processed. For more information, refer to Email processing logs (page 49).
- Status of software updates. For more information, refer to Antivirus and anti-spam engine updates (page 51).
- Log of POP2Exchange activities. For more information, refer to POP2Exchange activity (page 52).

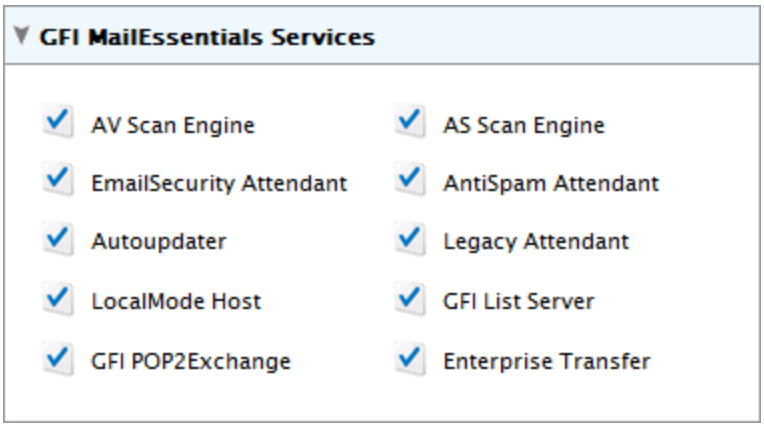
4.1.1 Status and statistics



Screenshot 10: The GFI MailEssentials Dashboard

To open the Dashboard, go to **GFI MailEssentials > Dashboard**. This page displays statistics, status of services and a graphical presentation of email activity. More details on these sections are provided below.

Services



Screenshot 11: The GFI MailEssentials Services

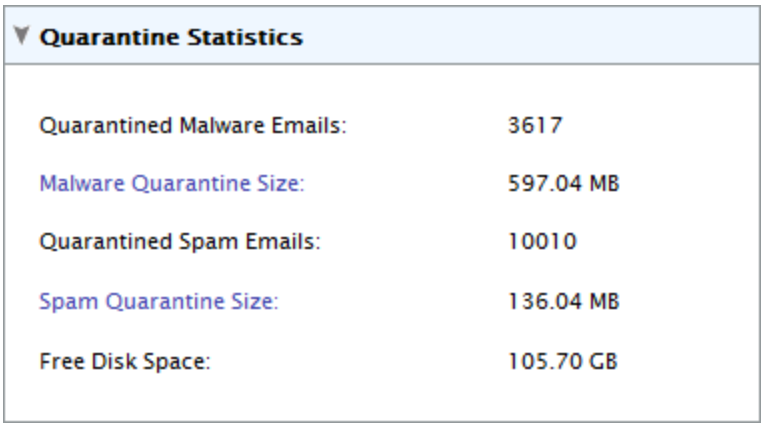
The **Services** area displays the status of GFI MailEssentials services.

» - Indicates that the service is started. Click this icon to stop service.

» - Indicates that the service is stopped. Click this icon to start a stopped service.

You can also start or stop services from the Microsoft® Windows Services console. To launch the Services console, go to **Start > Run**, type `services.msc` and click **OK**.

Quarantine Statistics

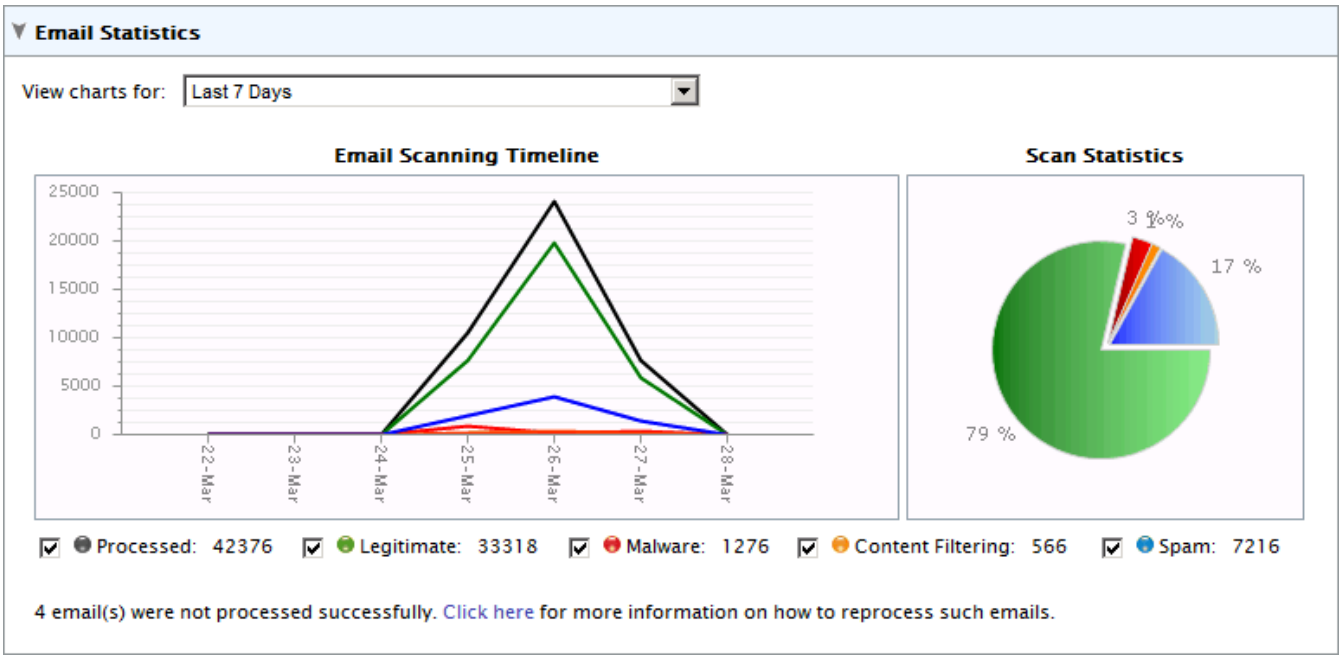

Quarantine Statistics
Quarantined Malware Emails: 3617
Malware Quarantine Size: 597.04 MB
Quarantined Spam Emails: 10010
Spam Quarantine Size: 136.04 MB
Free Disk Space: 105.70 GB

Screenshot 12: Quarantine statistics

The **Quarantine Statistics** area displays the following statistical information:

Statistic title	Description
Quarantined Malware Emails	Number of emails blocked by Email Security and Content Filtering engines, and stored in the Malware Quarantine Store.
Malware Quarantine Size	Size on disk of the Malware Quarantine Store database.
Quarantined Spam Emails	Number of emails blocked by anti-spam engines and stored in the Spam Quarantine Store.
Spam Quarantine Size	Size on disk of the Spam Quarantine Store database.
Free disk space	Free space on the disk where quarantine stores are saved.

Charts

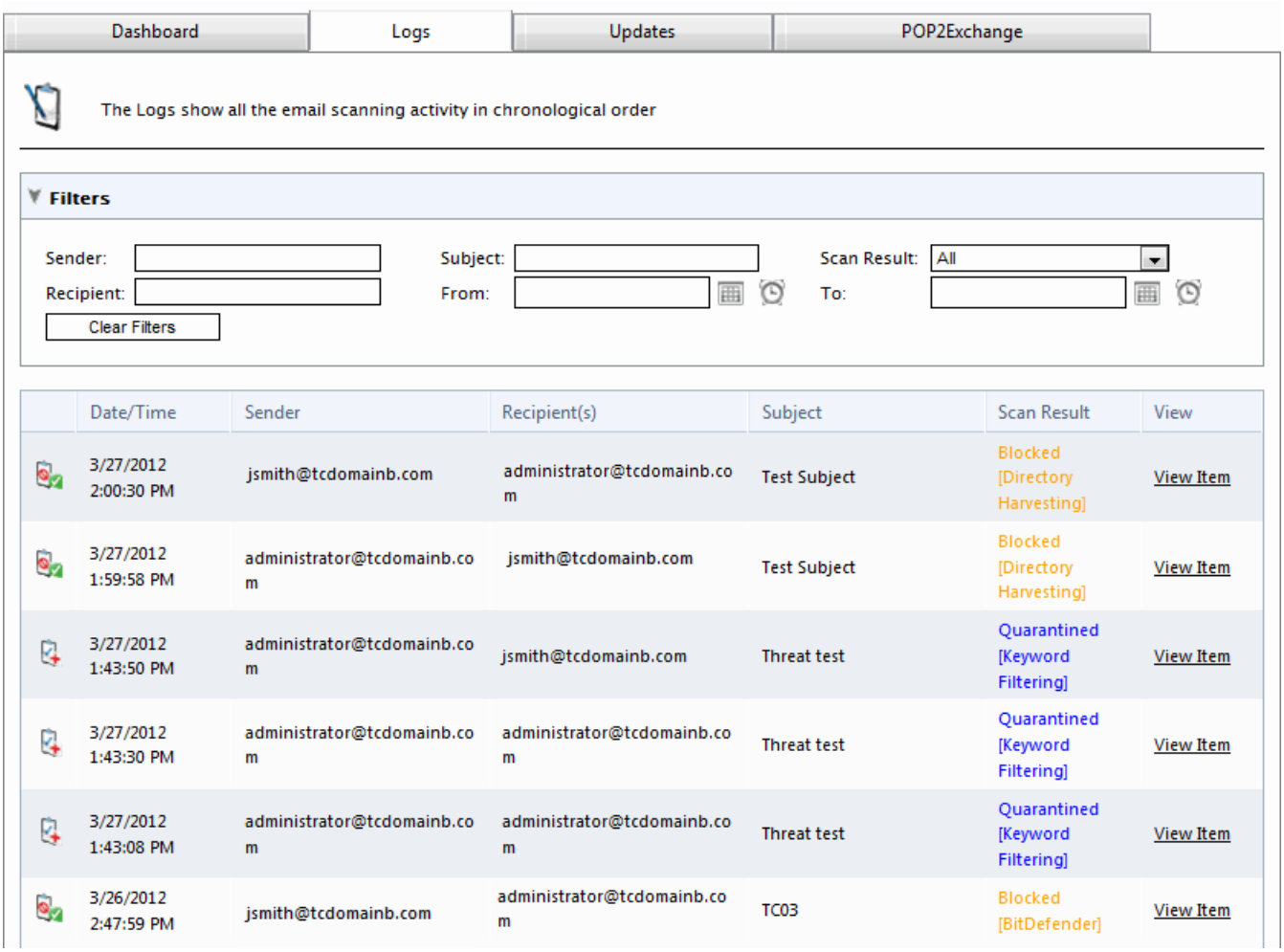


Screenshot 13: Dashboard charts

The **Charts** area displays graphical information about emails processed by GFI MailEssentials. Select the time period from the drop-down list to display information for that period in the charts.

Area	Description
View charts for	Enables you to select a period for which to view charts. Available options are: » Last 6 hours » Last 24 hours » Last 48 hours » Last 7 days
Email scanning timeline (time graph)	Shows a time graph in intervals for the time period selected. The graph shows the number of processed, legitimate, malware, content filtering and spam emails.
Scan statistics (pie chart)	A graphical distribution of the total number of safe, quarantined and failed emails for the time period selected.
Legend	The legend shows the color used in graphs and the count of each category.

4.1.2 Email processing logs



Screenshot 14: Email processing logs

From GFI MailEssentials Configuration, you can monitor all processed emails in real time. Navigate to **GFI MailEssentials > Dashboard** and select the **Logs** tab to display the list of processed emails. The following details are displayed for each email processed:

- Date/Time
- Sender
- Recipient(s)
- Subject
- Scan Result - shows the action taken on the email.

Action	Description
OK	Email is not blocked by GFI MailEssentials, and is delivered to its intended recipients.
Quarantined	Email is blocked by an engine or a filter that has the action set to Quarantine. Click **Quarantine** to review the email. **NOTE** The email cannot be previewed in quarantine if it was manually deleted from quarantine.
Blocked	Email is blocked by an engine or filter. Action taken is as configured for that particular engine.
Deleted	Email is blocked by an engine or filter with the action set to delete detected emails.

Action	Description
Failed	Email that could not be scanned by GFI MailEssentials. Email is moved to one of the following folder: *<GFI MailEssentials installation path>*\GFI\MailEssentials\EmailSecurity\FailedMails\ *<GFI MailEssentials installation path>*\GFI\MailEssentials\AntiSpam\FailedMails\ For more information, refer to Failed emails (page 231).

Filtering the email processing logs

Screenshot 15: Email processing logs filter

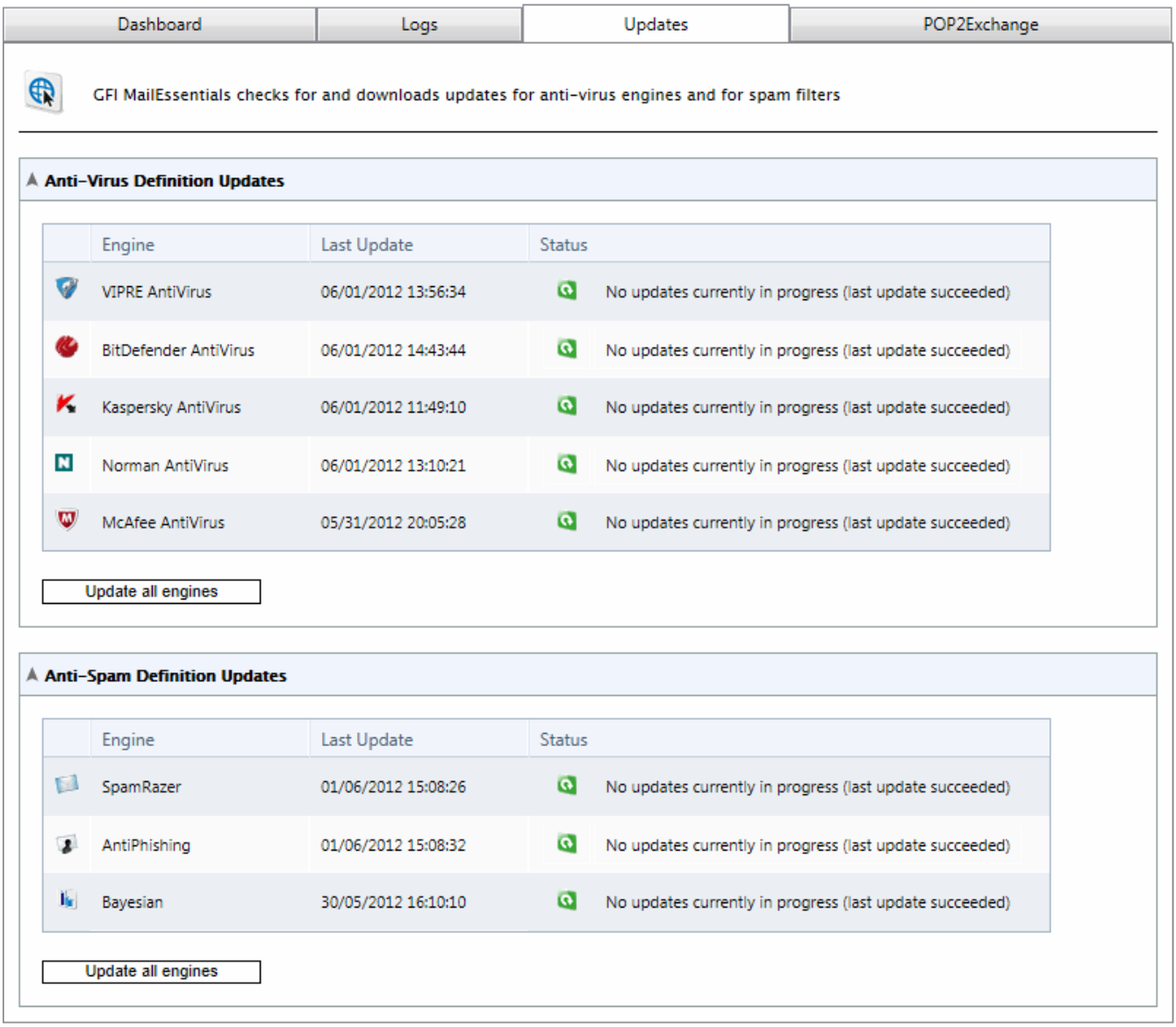
Filtering the email processing logs simplifies the reviewing process by providing the possibility to find particular emails. From the **Filter** area, specify any of the following criteria:

Filter	Description
Sender	Specify the full or part of an email address to display only the emails sent by matching senders.
Recipient	Specify the full or part of an email address to display only the emails sent to matching recipients.
Subject	Specify the full or part of an email subject to display only the emails with a matching subject.
Scan result	From the drop-down list, select whether to display only emails with a particular scan result (for example, quarantined emails only)
From & To	Specify a date and time range to display emails processed during that particular period.

NOTE

Click **Clear Filters** to remove specified filters and to show all email logs.

4.1.3 Antivirus and anti-spam engine updates



Screenshot 16: Virus scanning engines updates

The updates of antivirus and antispam scanning engines can be monitored from a central page. Go to **GFI MailEssentials > Dashboard** and select the **Updates** tab to review the status and dates when scanning engines were last updated.

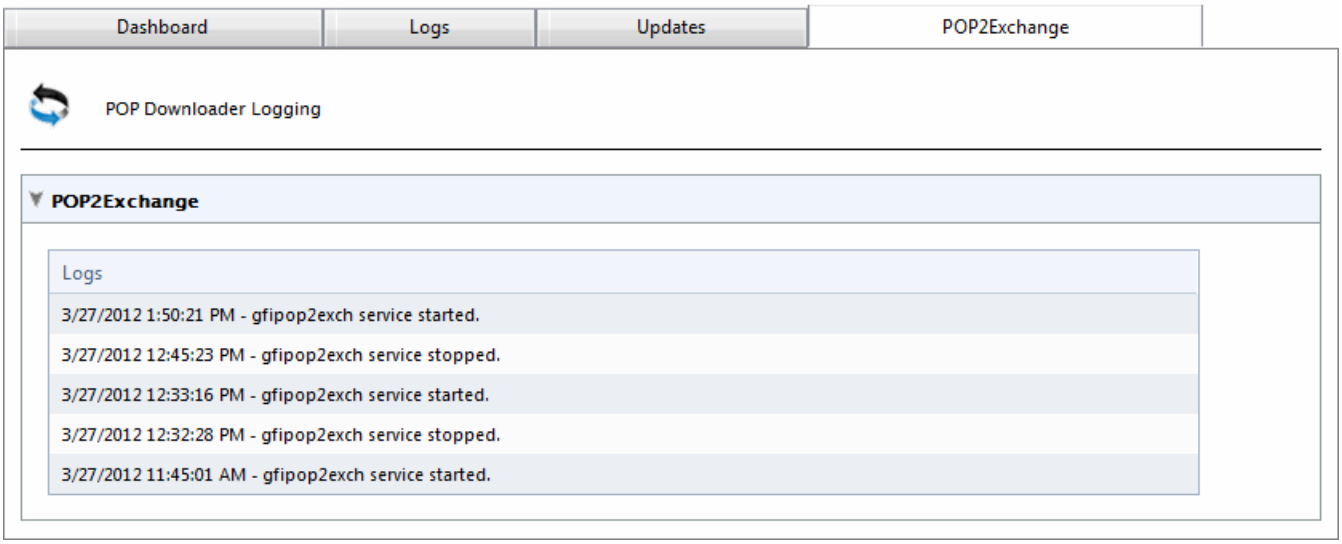
Click **Update all engines** to check for, and download, all updates.

The updates are checked for, and downloaded, as configured in the engines' configuration pages. Go to the configuration page of each engine and navigate to the **Updates** tab to configure update settings.

NOTE

Updates for each engine are checked for and downloaded sequentially (one engine update at a time).

4.1.4 POP2Exchange activity



Screenshot 17: POP2Exchange log

From GFI MailEssentials, you can monitor the activity of POP2Exchange in real time. Navigate to **GFI MailEssentials > Dashboard** and select the **POP2Exchange** tab.

NOTE

For more information, refer to POP2Exchange - Download emails from POP3 server (page 235).

4.2 Reports

GFI MailEssentials enables you to create reports based on data logged to database.

To access Reporting, go to **GFI MailEssentials > Reporting**.

- **Enabling reporting** - For more information, refer to Enabling/Disabling reporting (page 52).
- **Configure reporting database** - For more information, refer to Configuring reporting database (page 58).
- **Generate reports** - For more information, refer to Generating a report (page 53).
- **Create custom reports** - For more information, refer to Custom reports (page 56).
- **Search the reporting database** - For more information, refer to Searching the reporting database (page 57).

4.2.1 Enabling/Disabling reporting

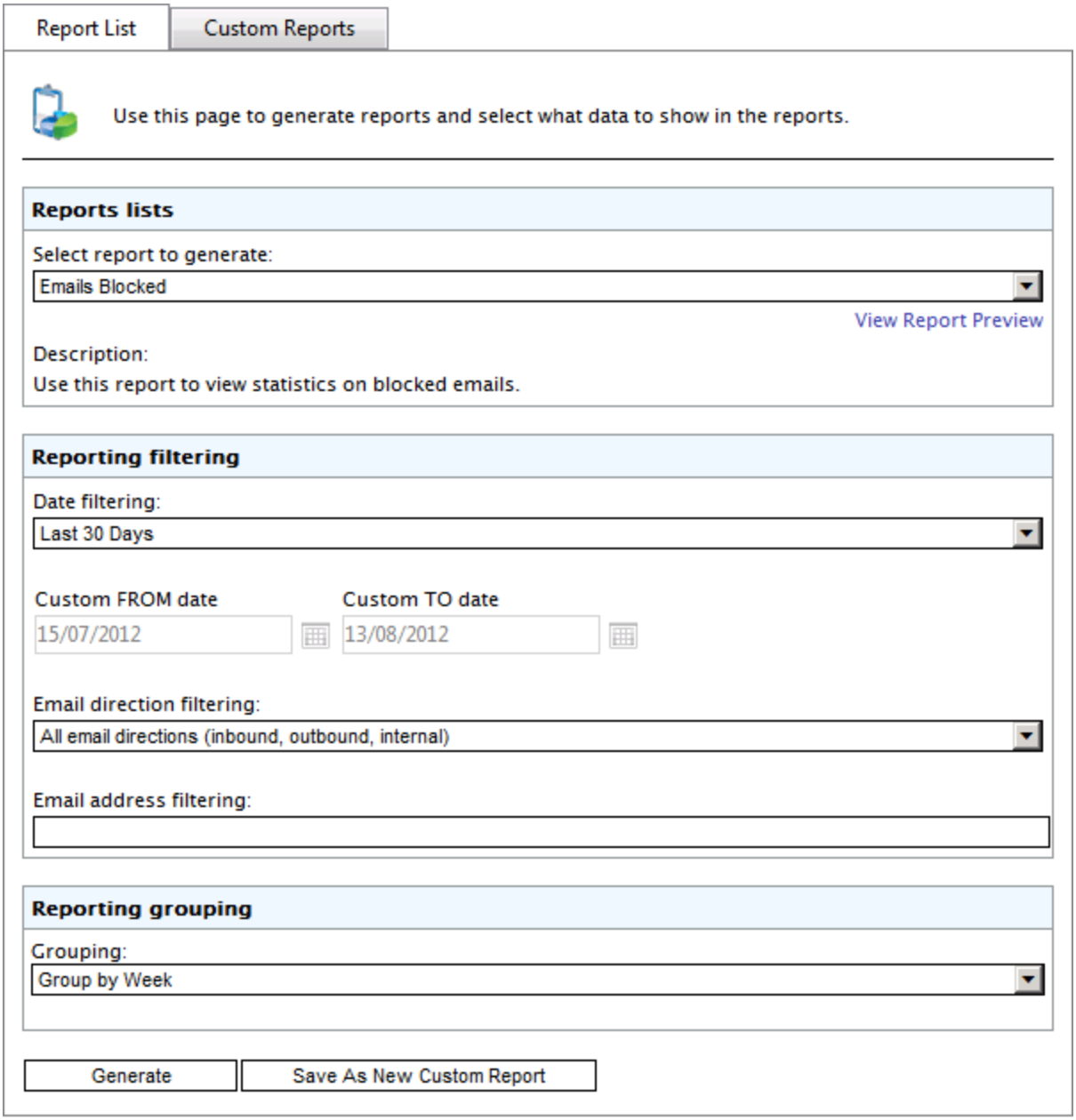
By default, Reporting is enabled and email activity data is logged to a Microsoft® Access database located in:

<GFI MailEssentials installation path>\GFI\MailEssentials\data\reports.mdb.

Go to **Reporting > Settings** node and check or uncheck **Enable Reporting** to enable or disable reporting respectively.

4.2.2 Generating a report

1. From GFI MailEssentials configuration, go to **GFI MailEssentials > Reporting > Reports**.

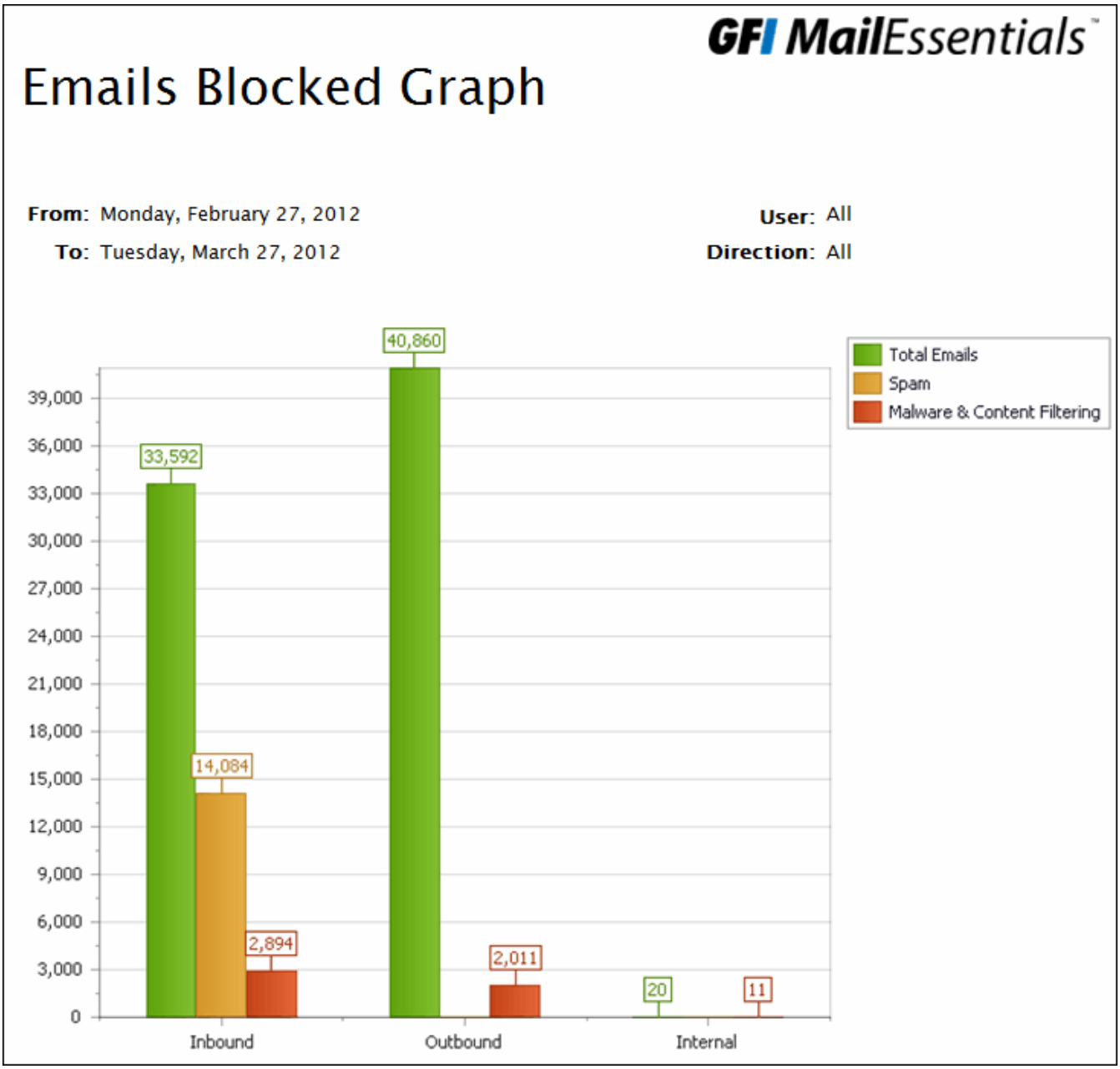


Screenshot 18: Creating a report

2. From the **Report List** tab, configure the following report options:

Option	Description
Report type	Select the type of report to generate: » **Emails Blocked** - shows total emails blocked by anti-spam and anti-malware filters for each email direction (Inbound, Outbound and Internal) out of all emails processed. » **Emails Blocked Graph** - graphically shows total emails blocked by anti-spam and anti-malware filters for each email direction (Inbound, Outbound and Internal) out of all emails processed. » **Email Direction Graph** - graphically shows total emails processed for each email direction - Inbound, Outbound and Internal. » **Email Direction** - shows total emails processed for each email direction - Inbound, Outbound and Internal. » **User Report** - shows the number of blocked and allowed emails for each email address. » **Spam Filter** - shows the total number of emails blocked by each anti-spam filter. » **Spam Filter Graph** - graphically shows the total number of emails blocked by each anti-spam filter. Click **View Report Preview** to preview how report looks like.
Date filtering	Select report date range. When selecting **Custom date range**, specify the period to display data for, from the **Custom From** and **Custom To** calendar controls.
Email directions filtering	Select a particular email direction to display data for or select **All email directions (inbound, outbound, internal)** to display data for all directions.
Email address filtering	Key in an email address to display report information for that particular email address only.
Report Grouping	Specify how to group data. Available options are: » **Group by Day** » **Group by Week** » **Group by Month** » **Group by Year**

3. Click **Generate** to build and display the report or **Save as New Custom Report** to save report settings for reuse at a later time.



Screenshot 19: Emails blocked graph report

Report functions

Use the report top toolbar to do the following functions:

Function	Icon	Description
Print		Click to print report.
Print current page		Click to print the page that is currently displayed.
Navigate		Use this toolbar to navigate through report pages.
Save		Select format to save report in and click **Save**. Specify location where to save report.

4.2.3 Custom reports

Custom reports enable you to save specific report parameters (for example, a report type for a specific time/date period) and to have it generated on a schedule. Use this feature to automate report generation.

Configuring custom reports

1. From GFI MailEssentials configuration, go to **GFI MailEssentials > Reporting > Reports**.
2. Select **Custom Reports** tab and click **New**.
3. Configure the following options:

Option	Description
Report type	Select the type of report to generate: » **Emails Blocked** - shows total emails blocked by anti-spam and anti-malware filters for each email direction (Inbound, Outbound and Internal) out of all emails processed. » **Emails Blocked Graph** - graphically shows total emails blocked by anti-spam and anti-malware filters for each email direction (Inbound, Outbound and Internal) out of all emails processed. » **Email Direction Graph** - graphically shows total emails processed for each email direction - Inbound, Outbound and Internal. » **Email Direction** - shows total emails processed for each email direction - Inbound, Outbound and Internal. » **User Report** - shows the number of blocked and allowed emails for each email address. » **Spam Filter** - shows the total number of emails blocked by each anti-spam filter. » **Spam Filter Graph** - graphically shows the total number of emails blocked by each anti-spam filter. Click **View Report Preview** to preview how report looks like.
Date filtering	Select report date range. When selecting **Custom date range**, specify the period to display data for, from the **Custom From** and **Custom To** calendar controls.
Email directions filtering	Select a particular email direction to display data for or select **All email directions (inbound, outbound, internal)** to display data for all directions.
Email address filtering	Key in an email address to display report information for that particular email address only.
Report Grouping	Specify how to group data. Available options are: » **Group by Day** » **Group by Week** » **Group by Month** » **Group by Year**

4. Optionally, enable **Send every** checkbox and configure a date/time combination to have the report generate at a specific date and time . Click **Add Rule** to save report generation time.

> **NOTE:**
> To delete a rule, select an existing report generation time and click **Delete**.

5. Select whether to send report by email or save it to disk. To send report by email, select **Send by email** and provide the email address to where the email is sent. To save report to disk,

select **Save to Disk**, provide a location where file will be saved the format of the file.

6. Click **Save** to save newly created report.

4.2.4 Generating custom reports

To generate a custom report:

1. From GFI MailEssentials configuration, go to **GFI MailEssentials > Reporting > Reports**.
2. From the **Custom Reports** tab, select a report to generate.
3. Click **Generate**.

4.2.5 Deleting custom reports

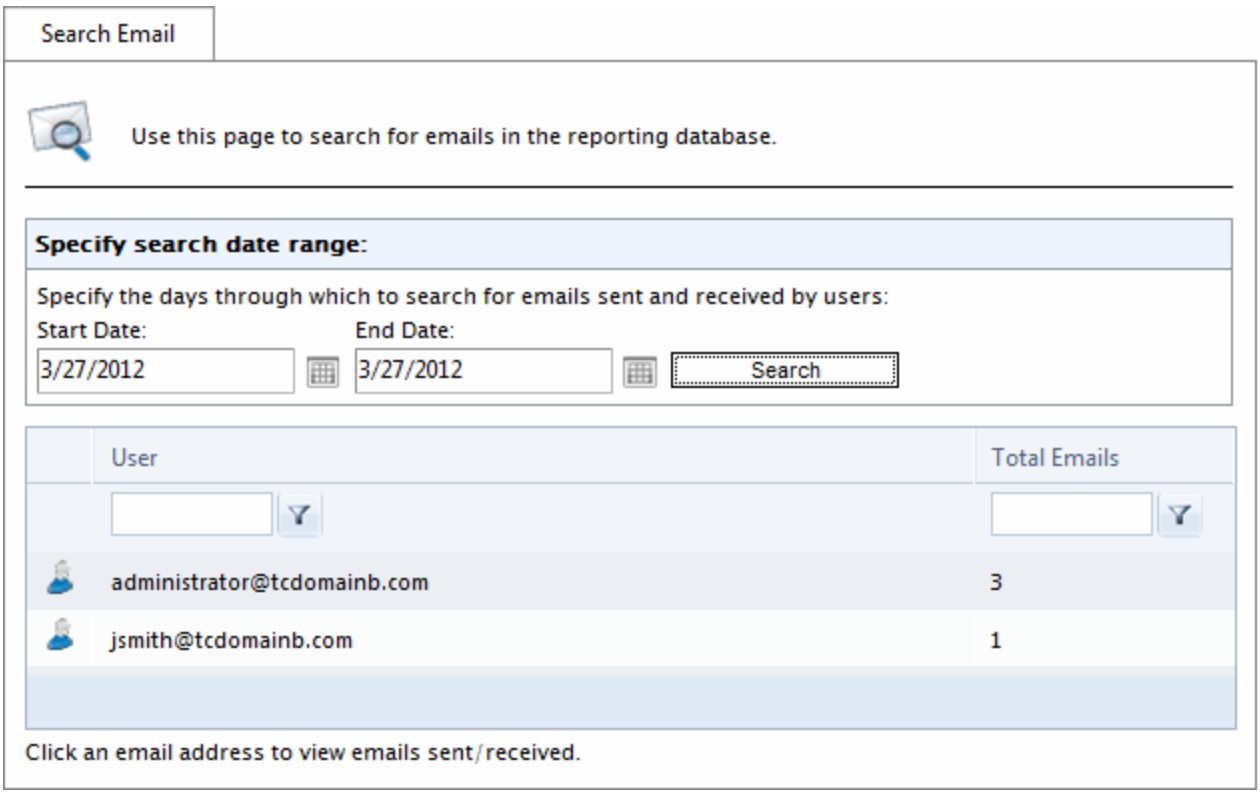
To delete a custom report:

1. From GFI MailEssentials configuration, go to **GFI MailEssentials > Reporting > Reports**.
2. From the **Custom Reports** tab, select a report to delete.
3. Click **Delete**.

4.2.6 Searching the reporting database

GFI MailEssentials stores some properties of all emails processed in the reporting database. GFI MailEssentials enables you to search the reporting database, to find processed emails. To search the reporting database:

1. From GFI MailEssentials Configuration, go to **GFI MailEssentials > Reporting > Search**.

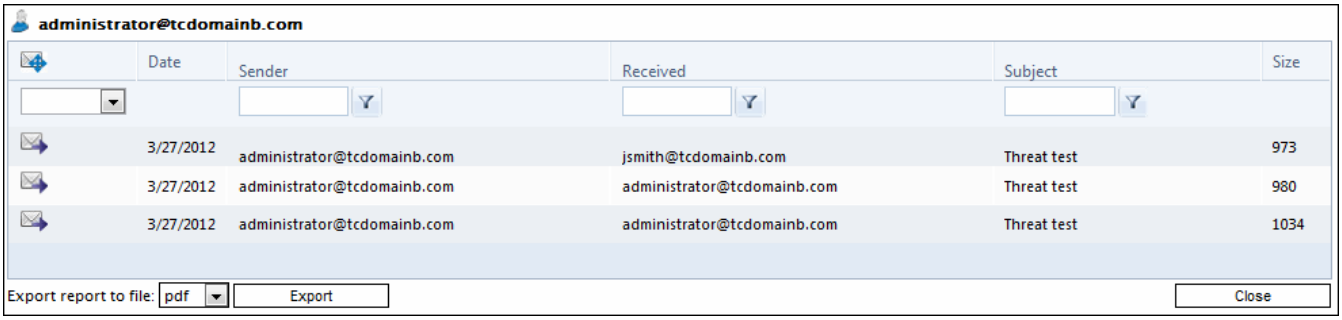


Screenshot 20: Searching the reporting database

2. Specify search criteria:

Search criteria	Description
Start date & End date	Select date range to filter emails from that period. Click **Search**.
User	Filter email address results. Key in number and click to specify conditions.
Total emails	Filter users by the amount of emails processed. Key in number and click to specify conditions.

3. The list of matching users is displayed. Click an email address to view detailed report of emails processed for that email address.



Screenshot 21: Reports database search results

4. (Optional) From the report, filter the data by email direction, sender, receiver or subject.

5. To export the report to another format, select format and click **Export**.

4.2.7 Configuring reporting database

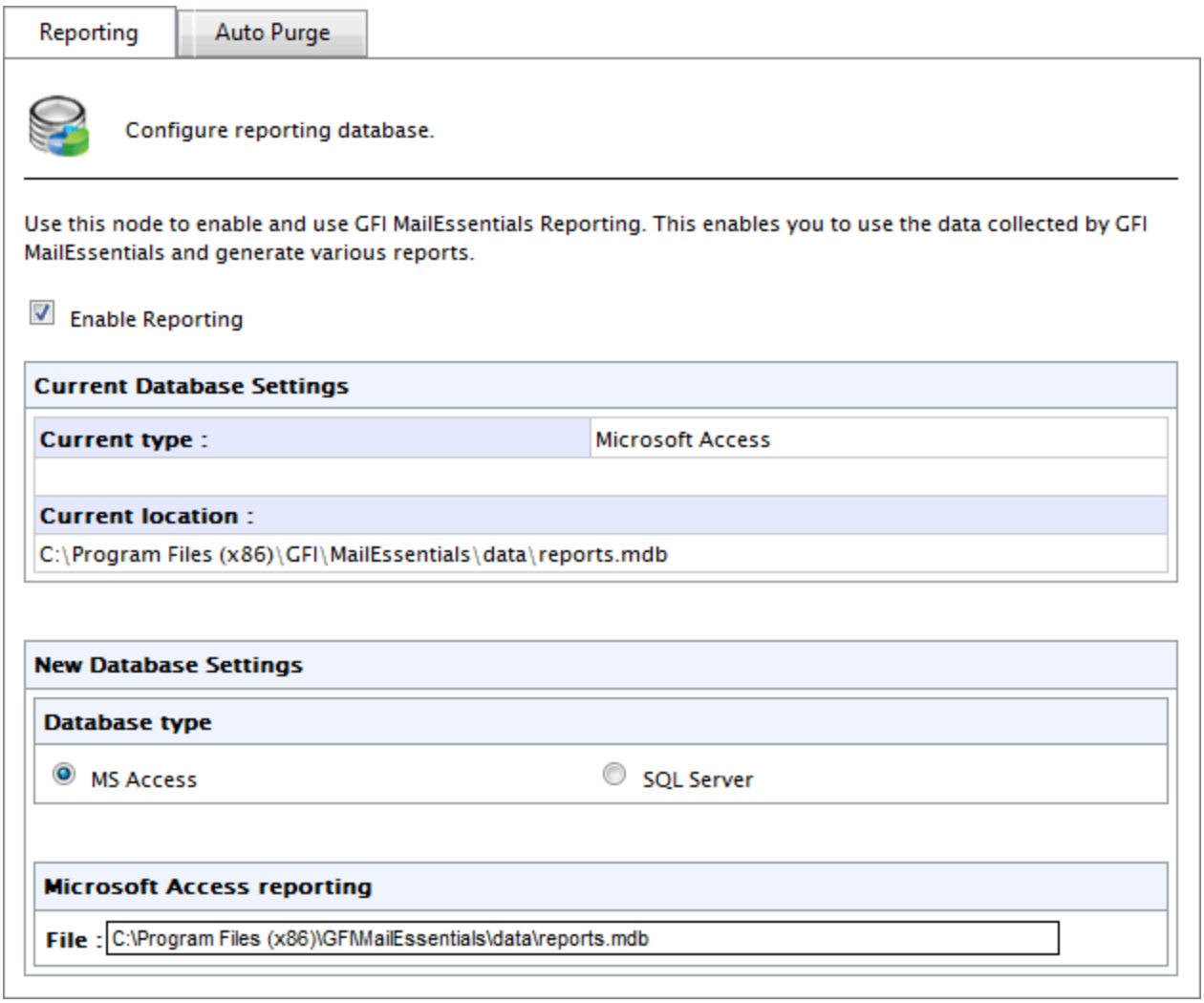
By default, GFI MailEssentials uses a Microsoft® Access database **reports.mdb** located in:

`<GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\data\`

You can also use a Microsoft® SQL Server database for reports.

- Configuring a Microsoft® Access database backend
- Configuring a Microsoft® SQL Server database backend
- Configuring database auto-purging

Configuring a Microsoft® Access database backend



Screenshot 22: Configuring a Microsoft® Access database backend

1. Navigate to **Reporting > Settings**.

2. Select **MS Access**.

3. Key in the complete path including filename (and .mdb extension) of the database file. If you only specify a filename, the database file is created in the following default path:

`<GFI MailEssentials installation path>\GFI\MailEssentials\data\`

4. Click **Apply**.

Configuring a Microsoft® SQL Server database backend

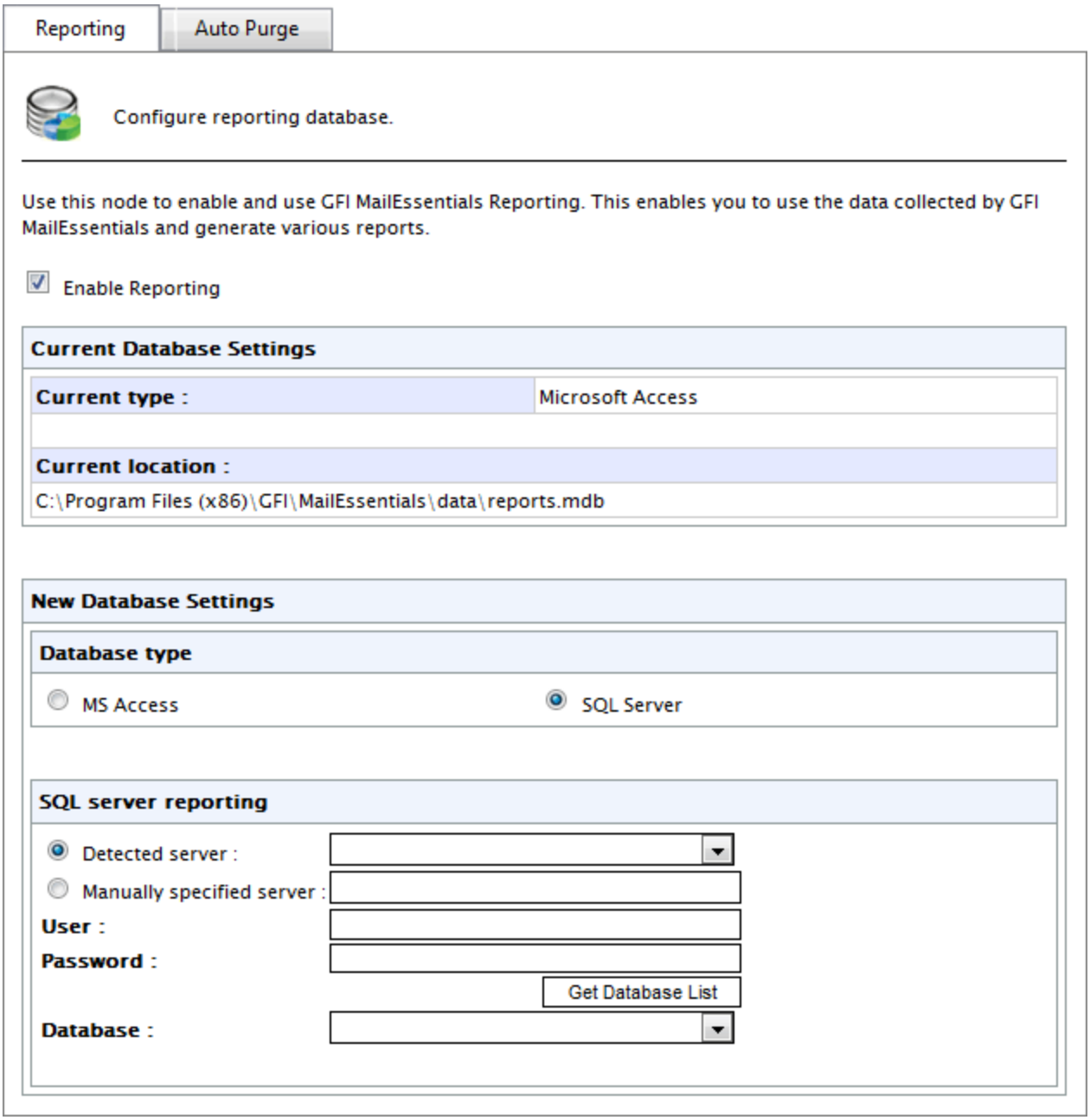
1. Create a new database in Microsoft® SQL Server.

> **NOTE**
>
> It is recommended to create a dedicated user/login in Microsoft® SQL Server for GFI MailEssentials and assign it the database owner role.

NOTE

For information how to create a new database in Microsoft® SQL Server refer to http://go.gfi.com/?pageid=ME_newSQLdb.

2. Navigate to **Reporting > Settings**.



Screenshot 23: Configuring SQL Server Database backend

3. Select **SQL Server**.

4. Select **Detected server** and select the automatically detected SQL Server from the list. If the server is not detected, select **Manually specified server** and key in the IP address or server name of the Microsoft® SQL Server.

5. Key in the credentials with permissions to read/write to the database.

6. Click **Get Database List** to extract the list of databases from the server.

7. From the **Database** list, select the database created for GFI MailEssentials Reporting.

8. Click **Apply**.

Configuring database auto-purging

You can configure GFI MailEssentials to automatically delete (auto-purge) records from the database that are older than a particular period. To enable auto-purging:

1. Navigate to **Reporting > Settings** and select **Auto-purge** tab.
2. Select **Enable Auto-Purging** and specify how long items in database should be stored in months .

> **NOTE**
>
> Auto-purging is applied only to the current database configured in the Reporting tab.

3. Click **Apply**.

5 User Actions

GFI MailEssentials uses Active Directory groups to determine what is displayed to logged in users when they login GFI MailEssentials. If the currently logged in user is part of the Administrators group, then GFI MailEssentials loads with all the configuration options that enable setting up GFI MailEssentials. If the currently logged in user is part of the users group, then GFI MailEssentials loads with only a limited number of options that enable the currently logged on user to administer his/her own quarantine and the personal whitelist/blocklists. The url used to login GFI MailEssentials is always the same one, regardless of whether the currently logged on user is part of the administrator or user Active Directory group.

This topic explains what users can do when they login using a user (non Active Directory Administrator) account.

> **NOTE:**
>
> User actions are only available if GFI MailEssentials is configured to use IIS mode. For more information, refer to User interface mode (page 227).

Topics in this chapter:

5.1 Personal Whitelist and Blocklist 62

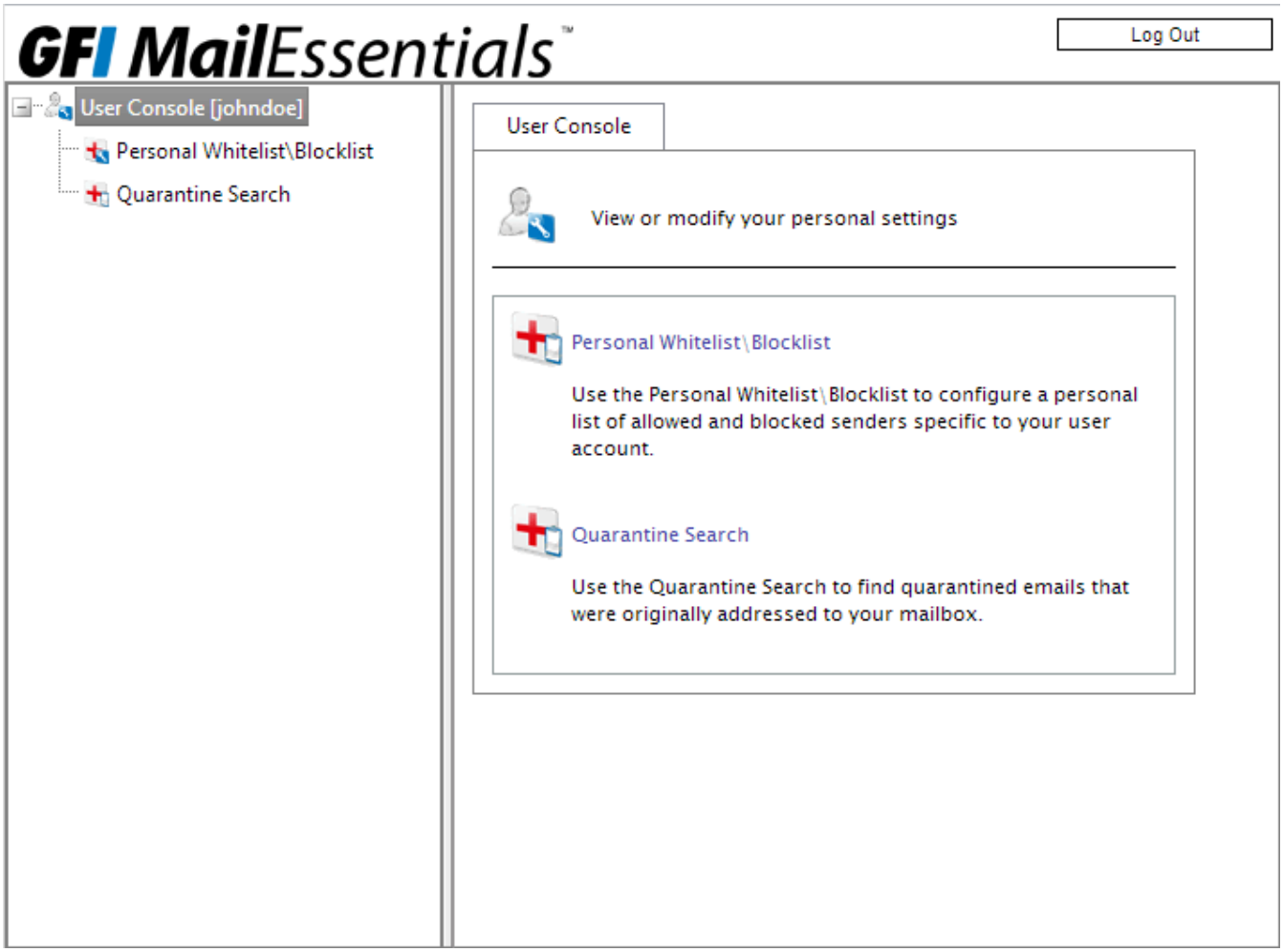
5.2 Quarantine Search 64

5.2.1 Using the Quarantine Search 65

5.1 Personal Whitelist and Blocklist

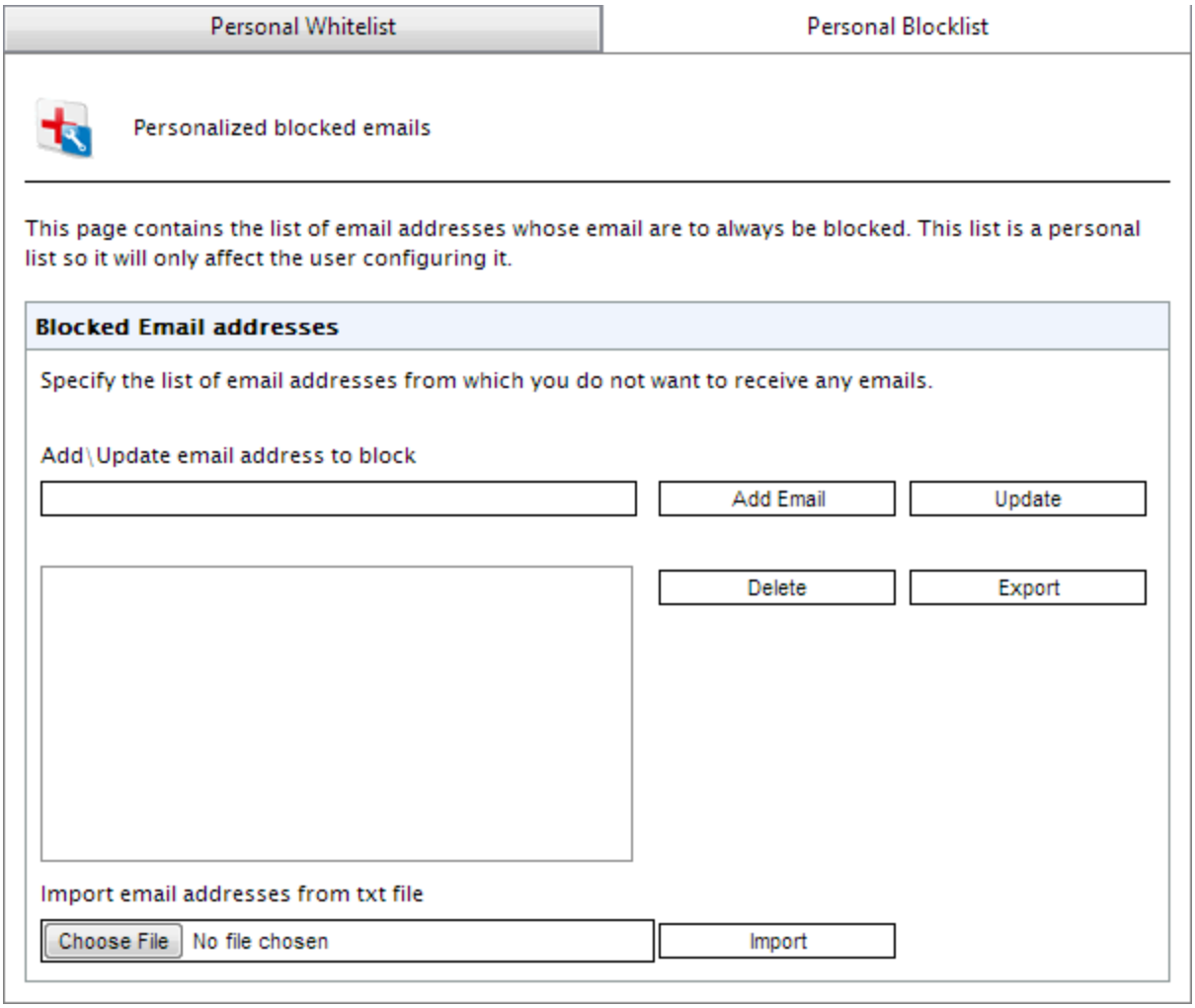
The Personal Whitelist and Blocklist feature enables users to configure a complimentary list of whitelisted and blocklisted email addresses, over and above the list set up by the systems administrator. To configure a Personal Whitelist/Blocklist:

1. Logon GFI MailEssentials using a user Active Directory or user logon credentials.


GFI MailEssentials
Log Out
User Console [johndoe]
Personal Whitelist\Blocklist
Quarantine Search
User Console
View or modify your personal settings
Personal Whitelist\Blocklist
Use the Personal Whitelist\Blocklist to configure a personal list of allowed and blocked senders specific to your user account.
Quarantine Search
Use the Quarantine Search to find quarantined emails that were originally addressed to your mailbox.

Screenshot 24: GFI MailEssentials logged on as a user

2. Select **Personal Whitelist\Blocklist.**


Personal Whitelist
Personal Blocklist
Personalized blocked emails
This page contains the list of email addresses whose email are to always be blocked. This list is a personal list so it will only affect the user configuring it.
Blocked Email addresses
Specify the list of email addresses from which you do not want to receive any emails.
Add\Update email address to block
Add Email
Update
Delete
Export
Import email addresses from txt file
Choose File
No file chosen
Import

Screenshot 25: Personal Whitelist\Blocklist

3. To create a Personal Whitelist, select **Personal Whitelist** tab; for personal blocklists, select **Personal Blocklist** tab.
4. Key in the email address to whitelist/block and click **Add Email**. To update an existing entry, select the email address, perform any required changes and click **Update**. To delete an exiting entry, select an entry and click **Delete**.

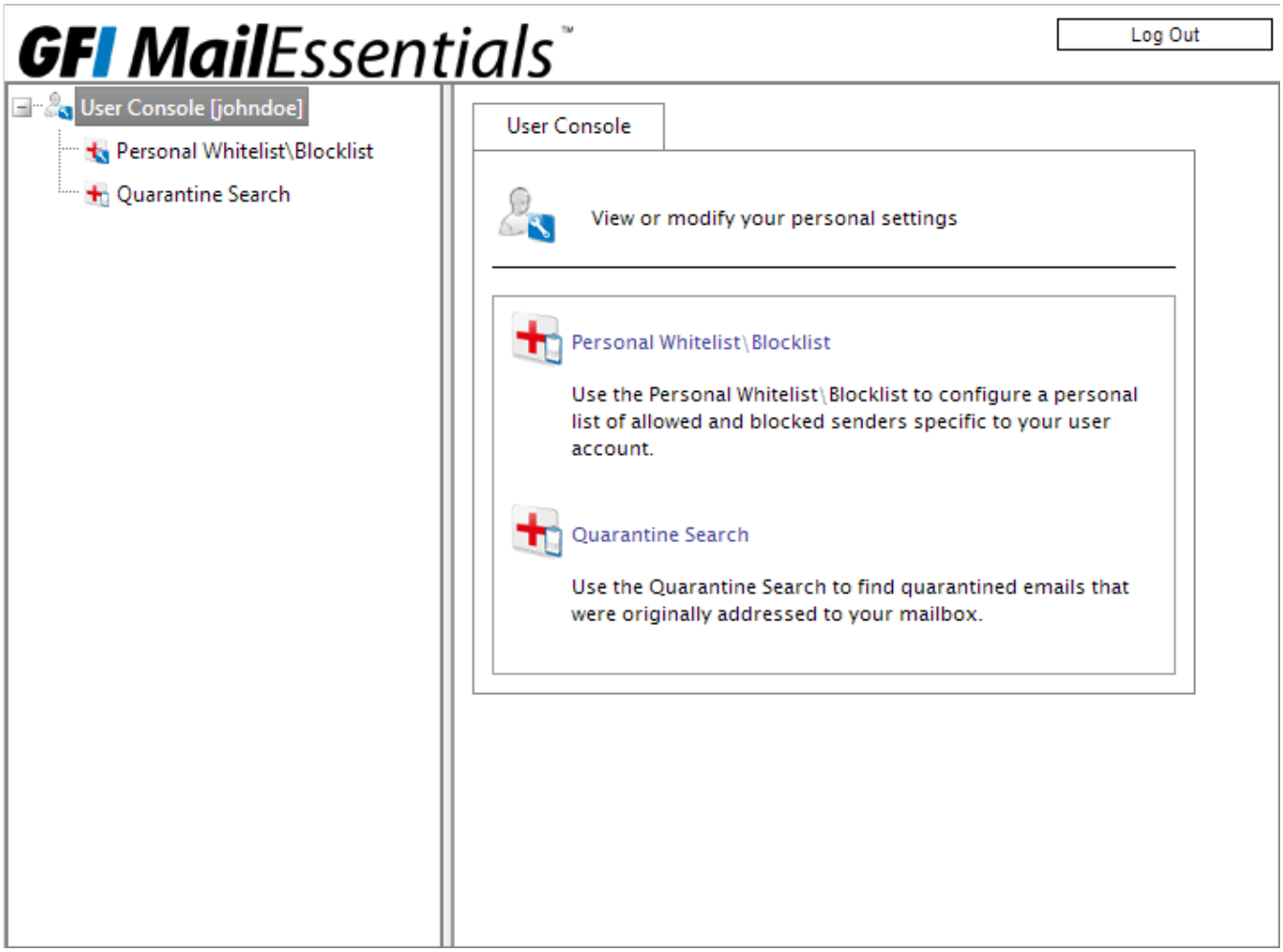
> **NOTE**
>
> You can also export and import lists. Click **Export** to export the current list of Whitelisted or Blocklisted emails. To import previously exported lists, click **Choose File**, select the exported file list and click **Import**.

5.2 Quarantine Search

The Quarantine Store is accessible from the GFI MailEssentials interface and allows management of quarantined emails. When logged in as a user, GFI MailEssentials provides the facility of searching and viewing through quarantined emails for the currently logged on user. Users can then approve or delete emails in quarantine.

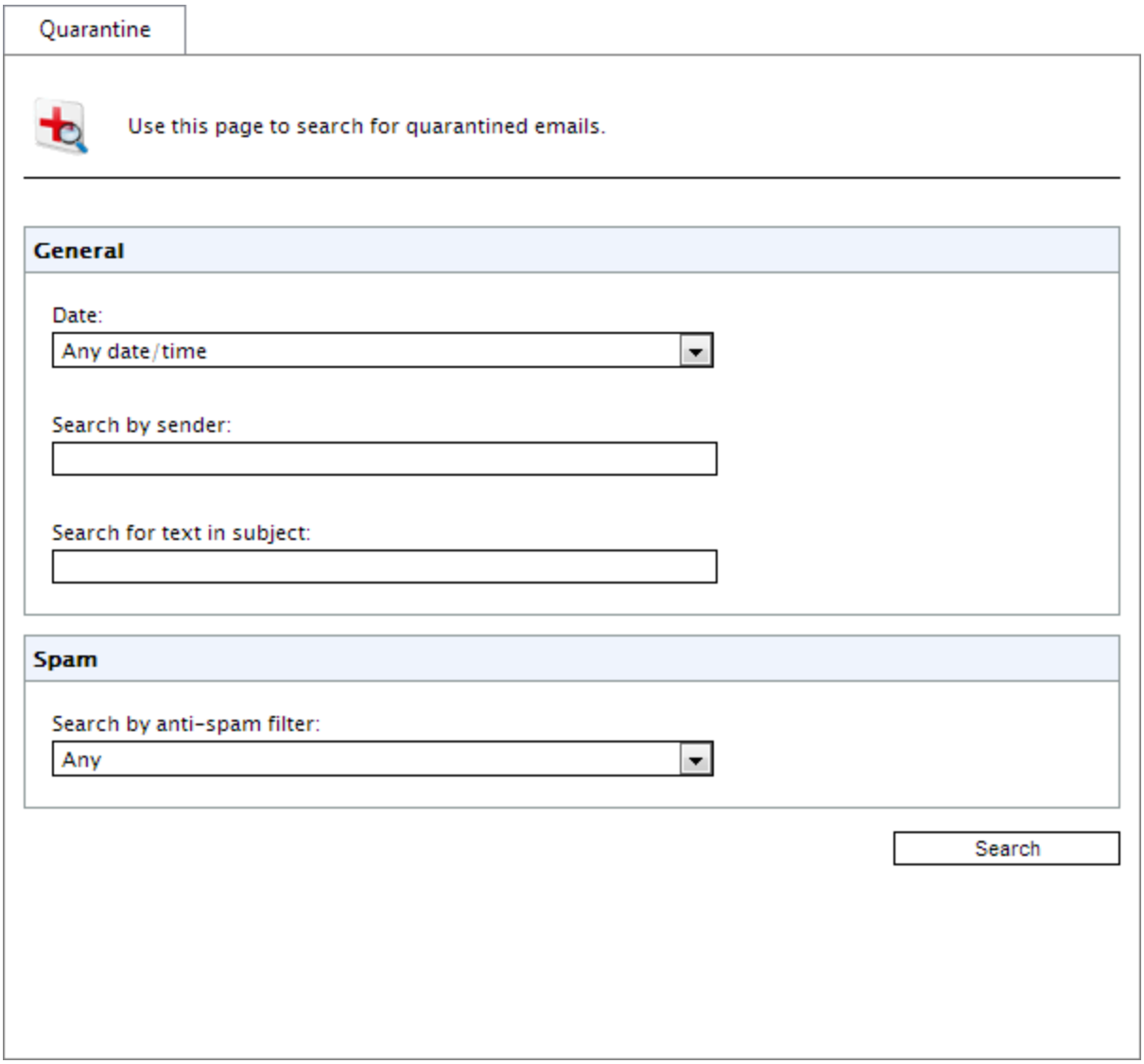
5.2.1 Using the Quarantine Search

1. Logon GFI MailEssentials using a user Active Directory or user logon credentials.


GFI MailEssentials
Log Out
User Console [johndoe]
Personal Whitelist\Blocklist
Quarantine Search
User Console
View or modify your personal settings
Personal Whitelist\Blocklist
Use the Personal Whitelist\Blocklist to configure a personal list of allowed and blocked senders specific to your user account.
Quarantine Search
Use the Quarantine Search to find quarantined emails that were originally addressed to your mailbox.

Screenshot 26: GFI MailEssentials logged on as a user

2. Select **Quarantine Search**.

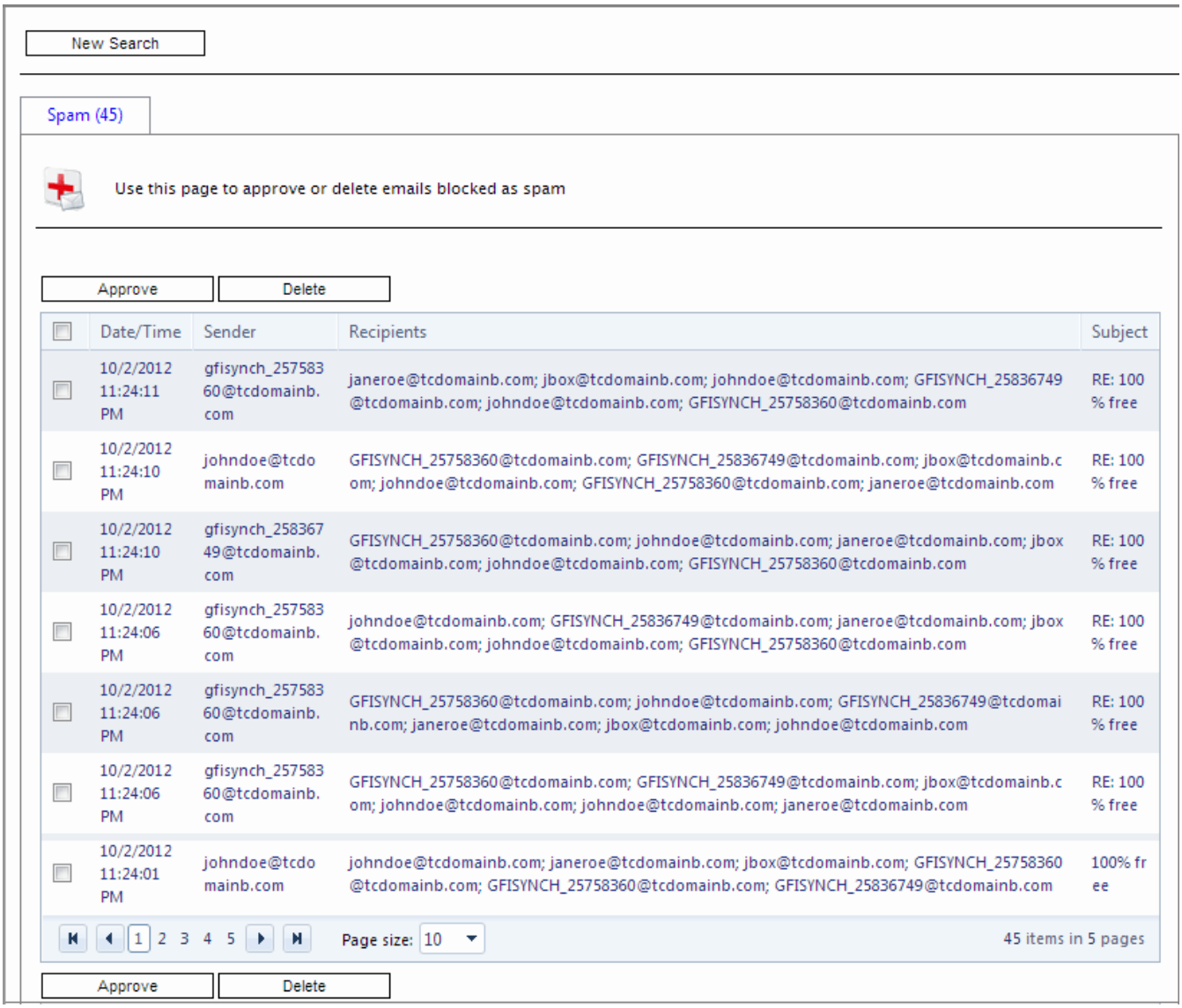


Screenshot 27: Quarantine Search

3. Specify the required search criteria.

SEARCH CRITERIA	DESCRIPTION
Date:	Select the date range when the email was quarantined. Available date ranges are: » Any date/time » Since yesterday » Last 7 days » Last 30 days » Custom date range
Search by sender	Specify a sender who sent the email that was quarantined.
Search for text in subject	Specify the text to search for within quarantined email subject.
Search by anti-spam filter	Select the filter that identified the email as spam.

4. Click **Search**.



Screenshot 28: Quarantine Search Results

5. Select one or more quarantined emails and click **Approve** to approve an email in mailbox and have it delivered to the currently logged on user's email. Alternatively click **Delete** to permanently delete an email from Quarantine.

6 Email Security

The security filters of GFI MailEssentials offer protection against virus-infected and other malicious emails.

Topics in this chapter:

6.1 Virus Scanning Engines 68

6.2 Information Store Protection 88

6.3 Trojan and Executable Scanner 91

6.4 Email Exploit Engine 94

6.5 HTML Sanitizer 97

6.1 Virus Scanning Engines

GFI MailEssentials uses multiple antivirus engines to scan inbound, outbound and internal emails for the presence of viruses. GFI MailEssentials ships with Vipre and BitDefender Virus Scanning Engines. You can also acquire a license for Norman, Kaspersky & McAfee.

This chapter describes how to configure Virus Scanning Engines, updates, actions and the scanning sequence.

6.1.1 Vipre 68

6.1.2 BitDefender 72

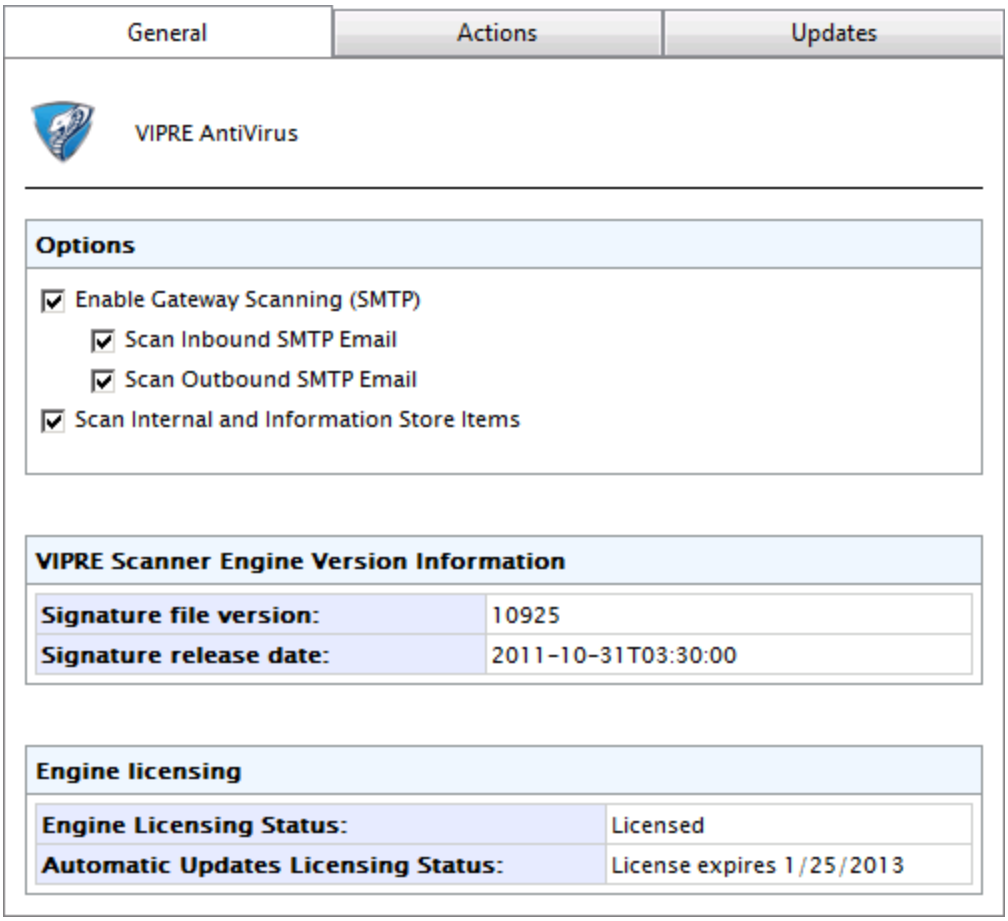
6.1.3 Kaspersky 76

6.1.4 Norman 79

6.1.5 McAfee 84

6.1.1 Vipre

1. Go to **Email Security > Virus Scanning Engines > Vipre.**



Screenshot 29: Vipre configuration

2. Select **Enable Gateway Scanning (SMTP)** check box, to scan emails using this Virus Scanning Engine.

3. Select whether to scan inbound and/or outbound emails using this Virus Scanning Engine.

Option	Description
Scan inbound SMTP email	Select this option to scan incoming emails
Scan outbound SMTP email	Select this option to scan outgoing emails

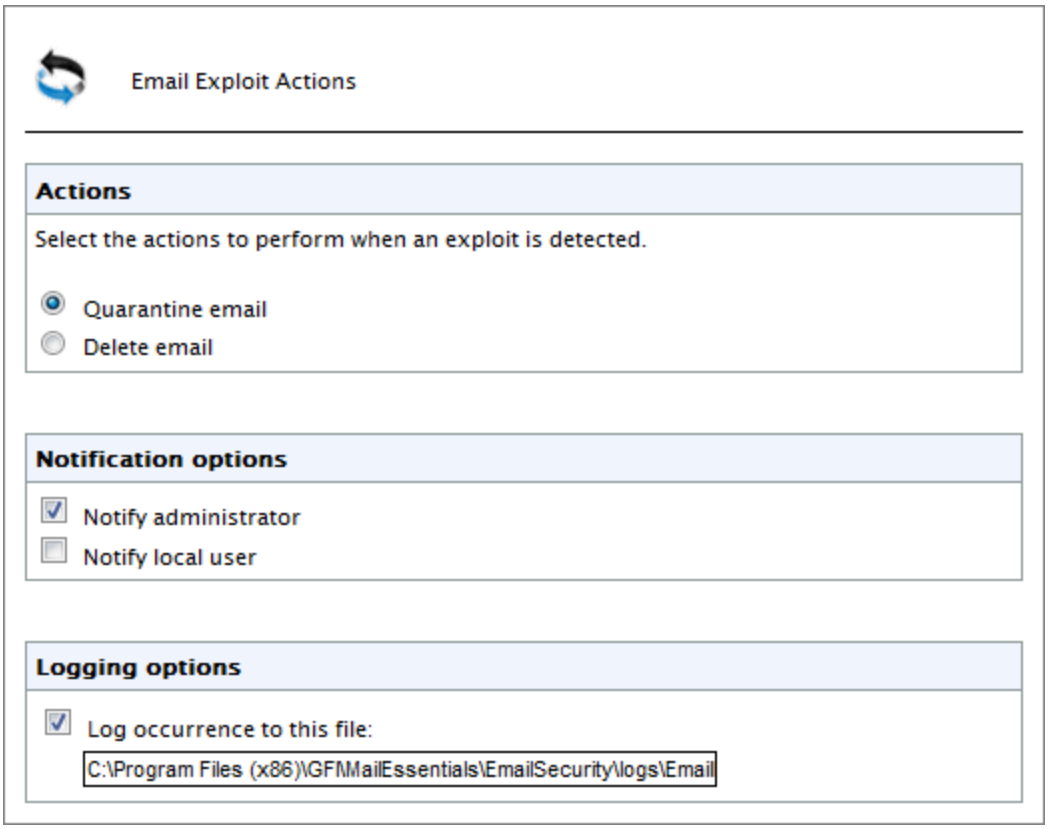
4. If you installed GFI MailEssentials on a Microsoft® Exchange machine, you will also have the option to scan internal emails and the Information Store. Select **Scan Internal and Information Store Items**.

NOTE

To use the Information Store Virus Scanning feature, you must enable the option from **Information Store Protection** node. For more information, refer to Information Store Protection (page 88).

NOTE

In this page you can also review the antivirus engine licensing and version information.



Screenshot 30: Virus scanning engine actions

5. From **Actions** tab, choose the action to take when an email is blocked:

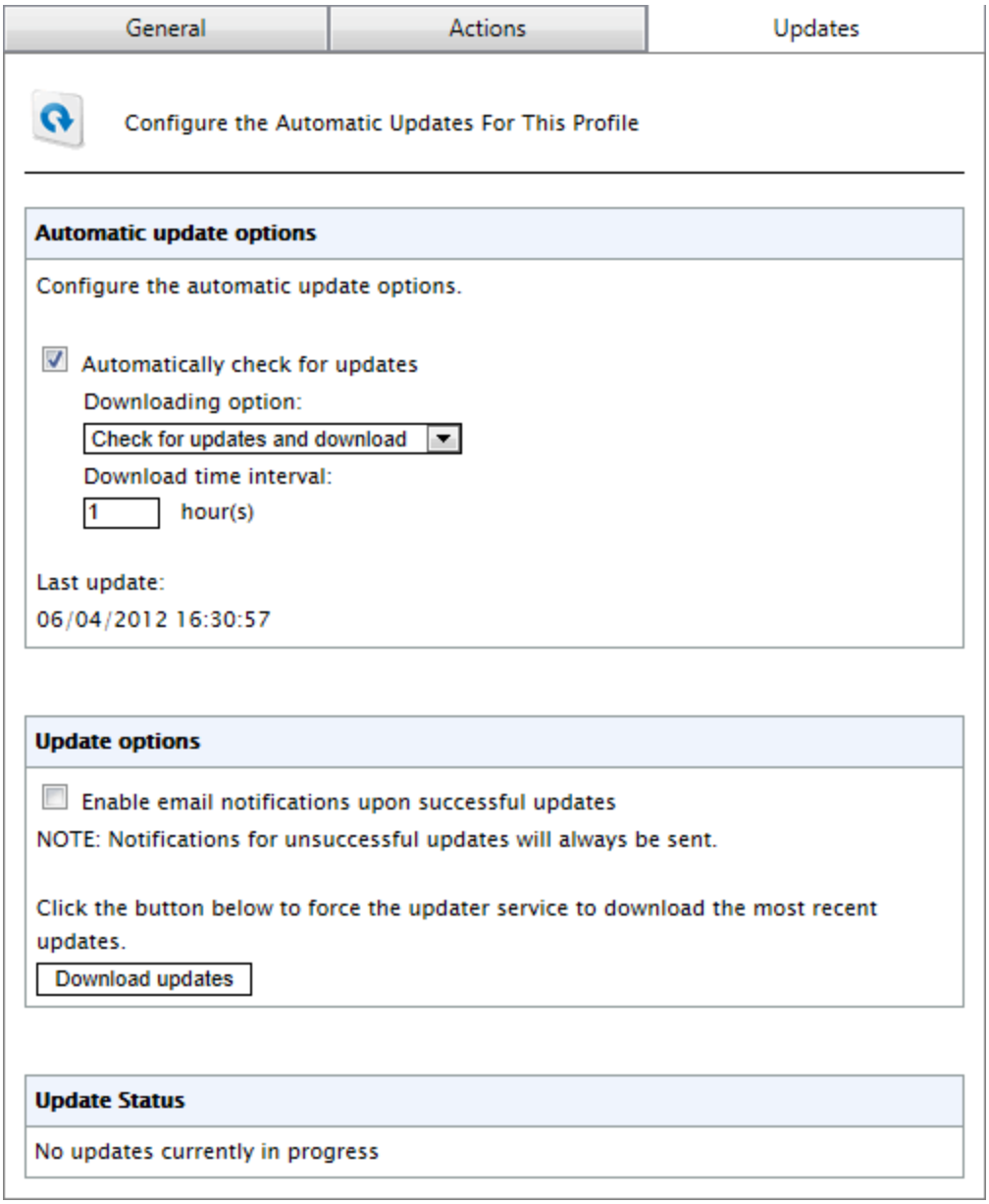
Action	Description
Quarantine email	Stores all infected emails detected by the selected Virus Scanning Engine in the Quarantine Store. You can subsequently review (approve/delete) all the quarantined emails. For more information, refer to Quarantine (page 180).
Delete email	Deletes infected emails.
Send a sanitized copy of the original email to recipient(s)	Choose whether to send a sanitized copy of the blocked email to the recipients.

6. GFI MailEssentials can send email notifications whenever an email triggers this filter. To enable this feature, select any of the following options:

Option	Description
Notify administrator	Notify the administrator whenever this engine blocks an email. For more information, refer to Administrator email address (page 219).
Notify local user	Notify the email local recipients about the blocked email.

7. To log the activity of this engine to a log file select **Log occurrence to this file**. In the text box specify path and file name to a custom location on disk where to store the log file. By default, log files are stored in:

```
<GFI MailEssentials installation
path>\GFI\MailEssentials\EmailSecurity\Logs\<EngineName>.log
```



Screenshot 31: Virus scanning engine updates

8. From **Updates** tab, select **Automatically check for updates** to enable automatic updating of the AV files for the selected engine.
9. From **Downloading option** list, select one of the following options:

Option	Description
Only check for updates	Select this option if you want GFI MailEssentials to just check for and notify the administrator when updates are available for this engine. This option will NOT download the available updates automatically.
Check for updates and download	Select this option if you want GFI MailEssentials to check for and automatically download any updates available for this engine.

10. Specify how often you want GFI MailEssentials to check/download updates for this engine, by specifying an interval value in hours.
11. From **Update options** area, select **Enable email notifications upon successful updates** to send an email notification to the administrator whenever the engine updates successfully.

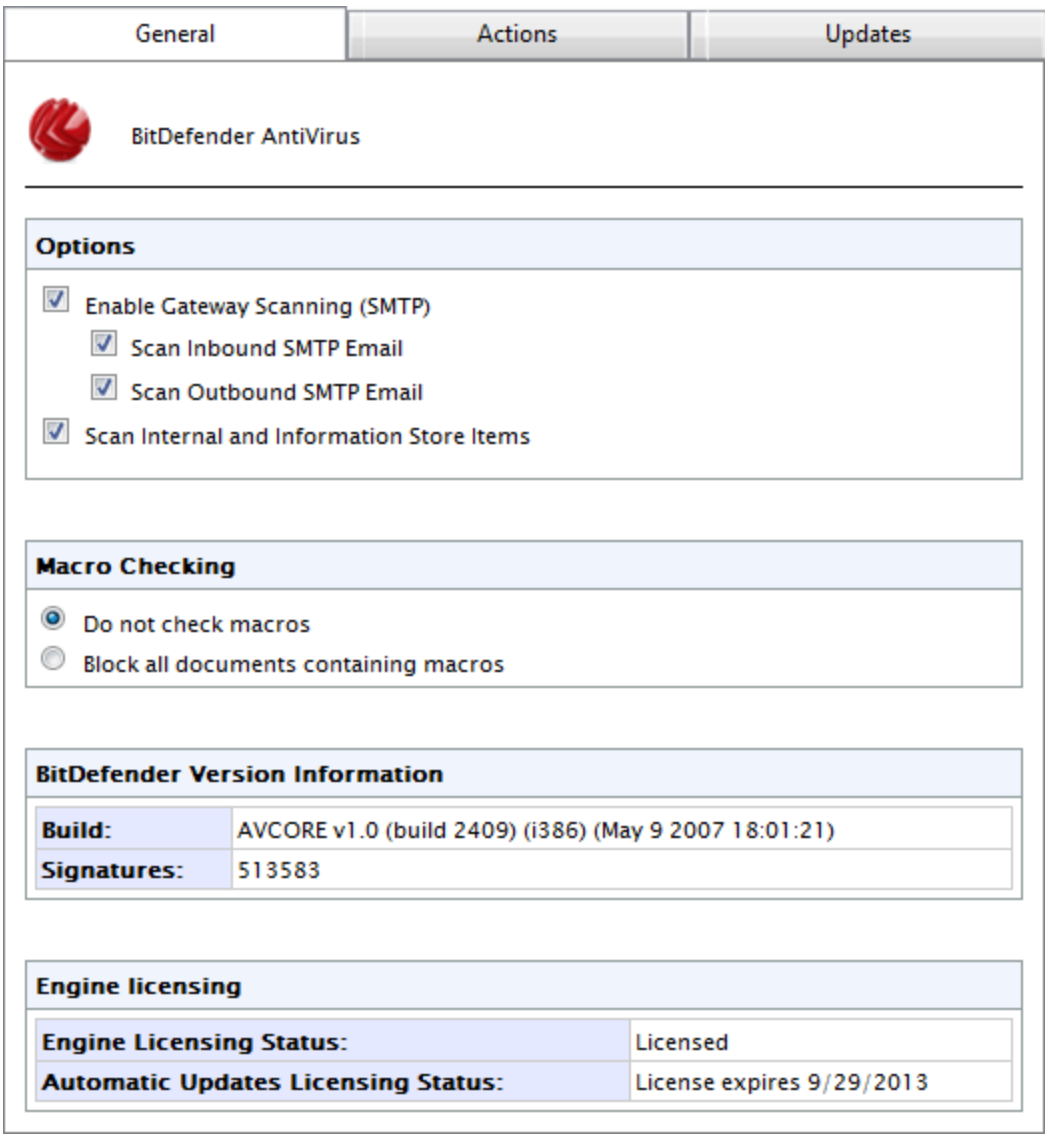
NOTE

An email notification is always sent when an update fails.

12. To check for and download updates immediately, click **Download updates**.
13. Click **Apply**.

6.1.2 BitDefender

1. Go to **Email Security > Virus Scanning Engines > BitDefender**.



Screenshot 32: BitDefender configuration

2. Select **Enable Gateway Scanning (SMTP)** check box, to scan emails using this Virus Scanning Engine.
3. Select whether to scan inbound and/or outbound emails using this Virus Scanning Engine.

Option	Description
Scan inbound SMTP email	Select this option to scan incoming emails
Scan outbound SMTP email	Select this option to scan outgoing emails

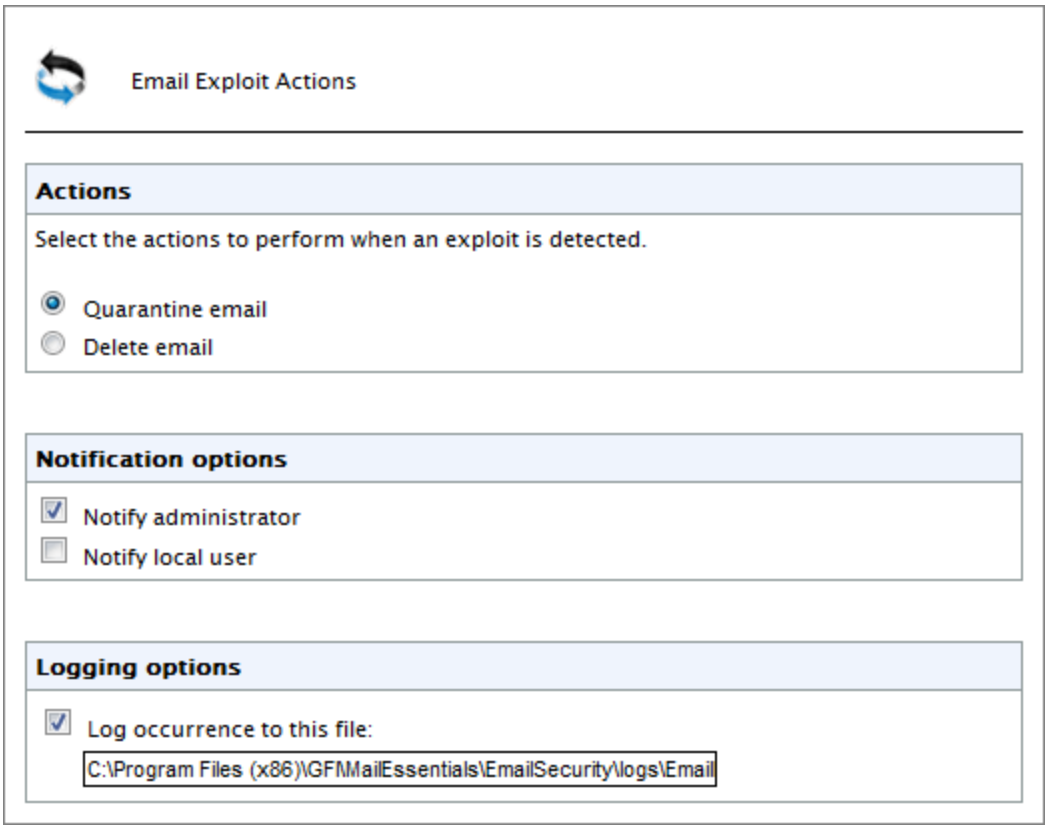
4. If you installed GFI MailEssentials on a Microsoft® Exchange machine, you will also have the option to scan internal emails and the Information Store. Select **Scan Internal and Information Store Items**.

> **NOTE**
>
> To use the Information Store Virus Scanning feature, you must enable the option from **Information Store Protection** node. For more information, refer to Information Store Protection (page 88).

> **NOTE**
>
> In this page you can also review the antivirus engine licensing and version information.

5. BitDefender can also be used to block emails with attachments that contain macros. Enable this feature from the **Macro Checking** area by selecting **Block all documents containing macros**.

> **NOTE**
>
> IF Macro Checking is disabled, GFI MailEssentials still scans for and blocks Macro Viruses.



Screenshot 33: Virus scanning engine actions

6. From **Actions** tab, choose the action to take when an email is blocked:

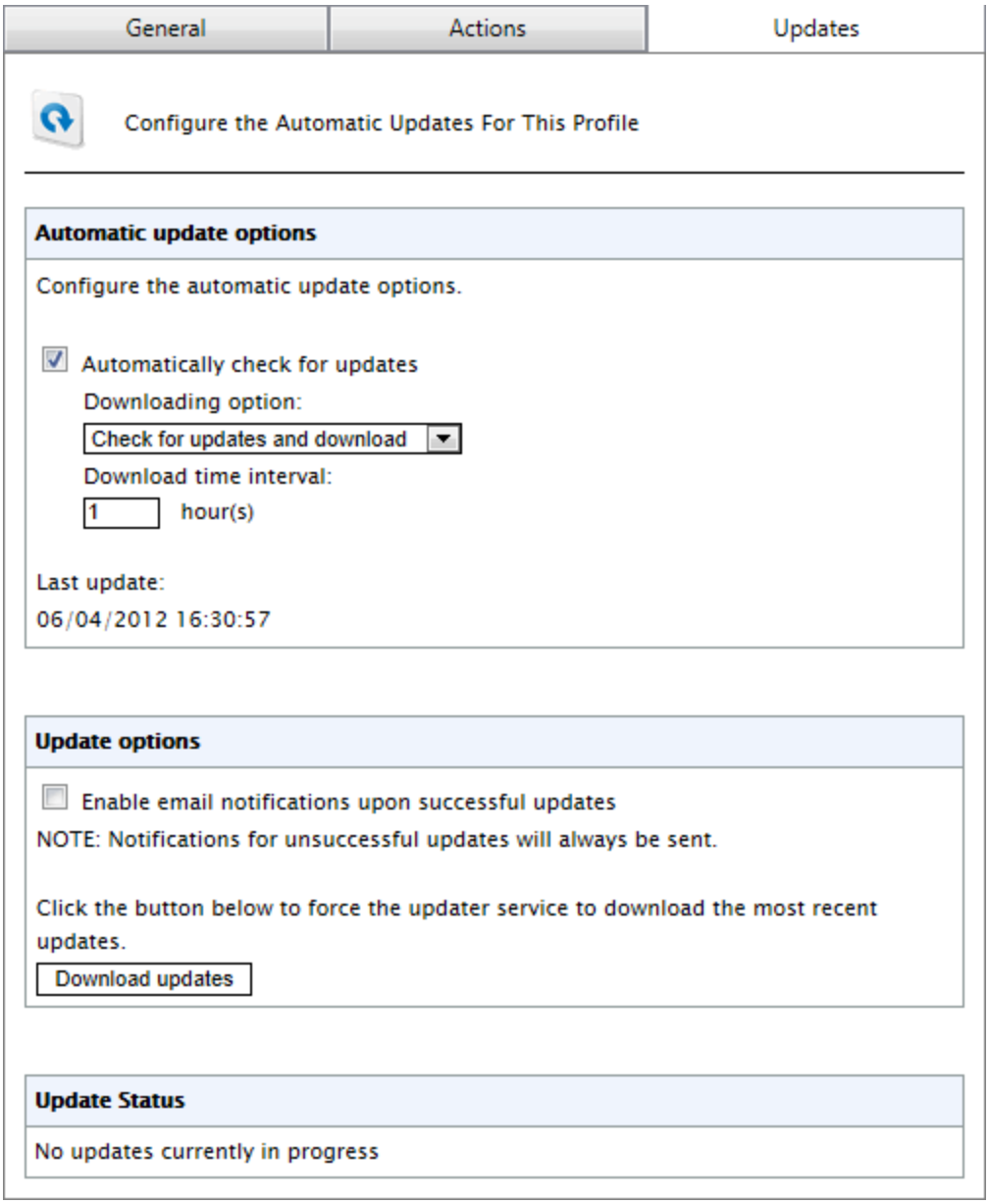
Action	Description
Quarantine email	Stores all infected emails detected by the selected Virus Scanning Engine in the Quarantine Store. You can subsequently review (approve/delete) all the quarantined emails. For more information, refer to Quarantine (page 180).
Delete email	Deletes infected emails.
Send a sanitized copy of the original email to recipient(s)	Choose whether to send a sanitized copy of the blocked email to the recipients.

7. GFI MailEssentials can send email notifications whenever an email triggers this filter. To enable this feature, select any of the following options:

Option	Description
Notify administrator	Notify the administrator whenever this engine blocks an email. For more information, refer to Administrator email address (page 219).
Notify local user	Notify the email local recipients about the blocked email.

8. To log the activity of this engine to a log file select **Log occurrence to this file**. In the text box specify path and file name to a custom location on disk where to store the log file. By default, log files are stored in:

```
<GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\Logs\<EngineName>.log
```



Screenshot 34: Virus scanning engine updates

9. From **Updates** tab, select **Automatically check for updates** to enable automatic updating of the AV files for the selected engine.

10. From **Downloading option** list, select one of the following options:

Option	Description
Only check for updates	Select this option if you want GFI MailEssentials to just check for and notify the administrator when updates are available for this engine. This option will NOT download the available updates automatically.
Check for updates and download	Select this option if you want GFI MailEssentials to check for and automatically download any updates available for this engine.

11. Specify how often you want GFI MailEssentials to check/download updates for this engine, by specifying an interval value in hours.

12. From **Update options** area, select **Enable email notifications upon successful updates** to send an email notification to the administrator whenever the engine updates successfully.

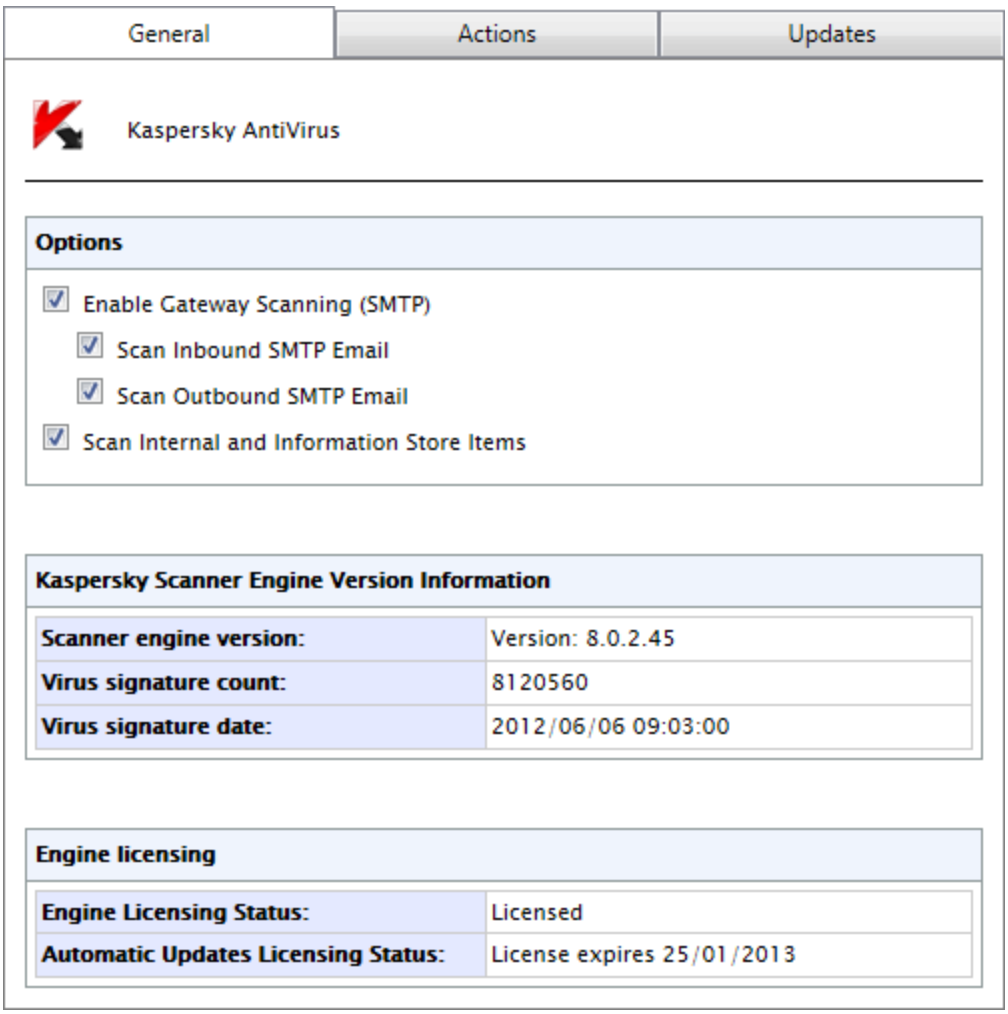
NOTE

An email notification is always sent when an update fails.

13. To check for and download updates immediately, click **Download updates**.
14. Click **Apply**.

6.1.3 Kaspersky

1. Go to **Email Security > Virus Scanning Engines > Kaspersky**.



Screenshot 35: Kaspersky configuration

2. Select **Enable Gateway Scanning (SMTP)** check box, to scan emails using this Virus Scanning Engine.
3. Select whether to scan inbound and/or outbound emails using this Virus Scanning Engine.

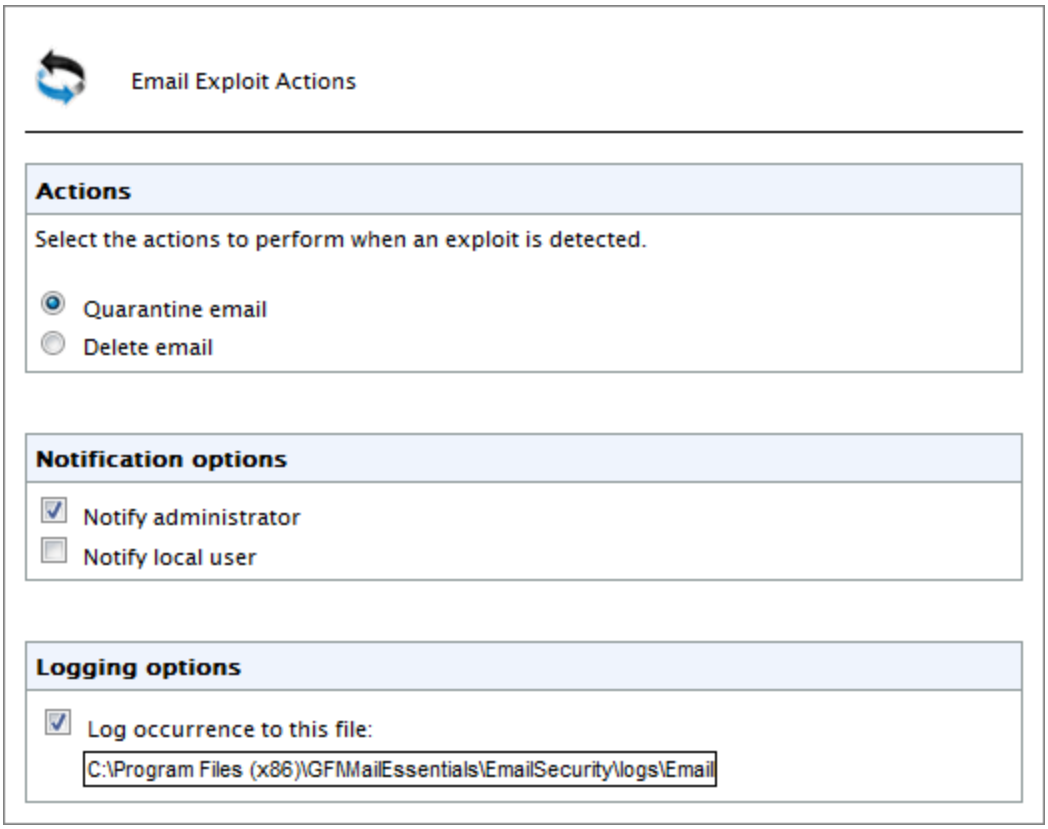
Option	Description
Scan inbound SMTP email	Select this option to scan incoming emails
Scan outbound SMTP email	Select this option to scan outgoing emails

4. If you installed GFI MailEssentials on a Microsoft® Exchange machine, you will also have the option to scan internal emails and the Information Store. Select **Scan Internal and Information**

Store Items.

> **NOTE**
>
> To use the Information Store Virus Scanning feature, you must enable the option from **Information Store Protection** node. For more information, refer to Information Store Protection (page 88).

> **NOTE**
>
> In this page you can also review the antivirus engine licensing and version information.



Screenshot 36: Virus scanning engine actions

5. From **Actions** tab, choose the action to take when an email is blocked:

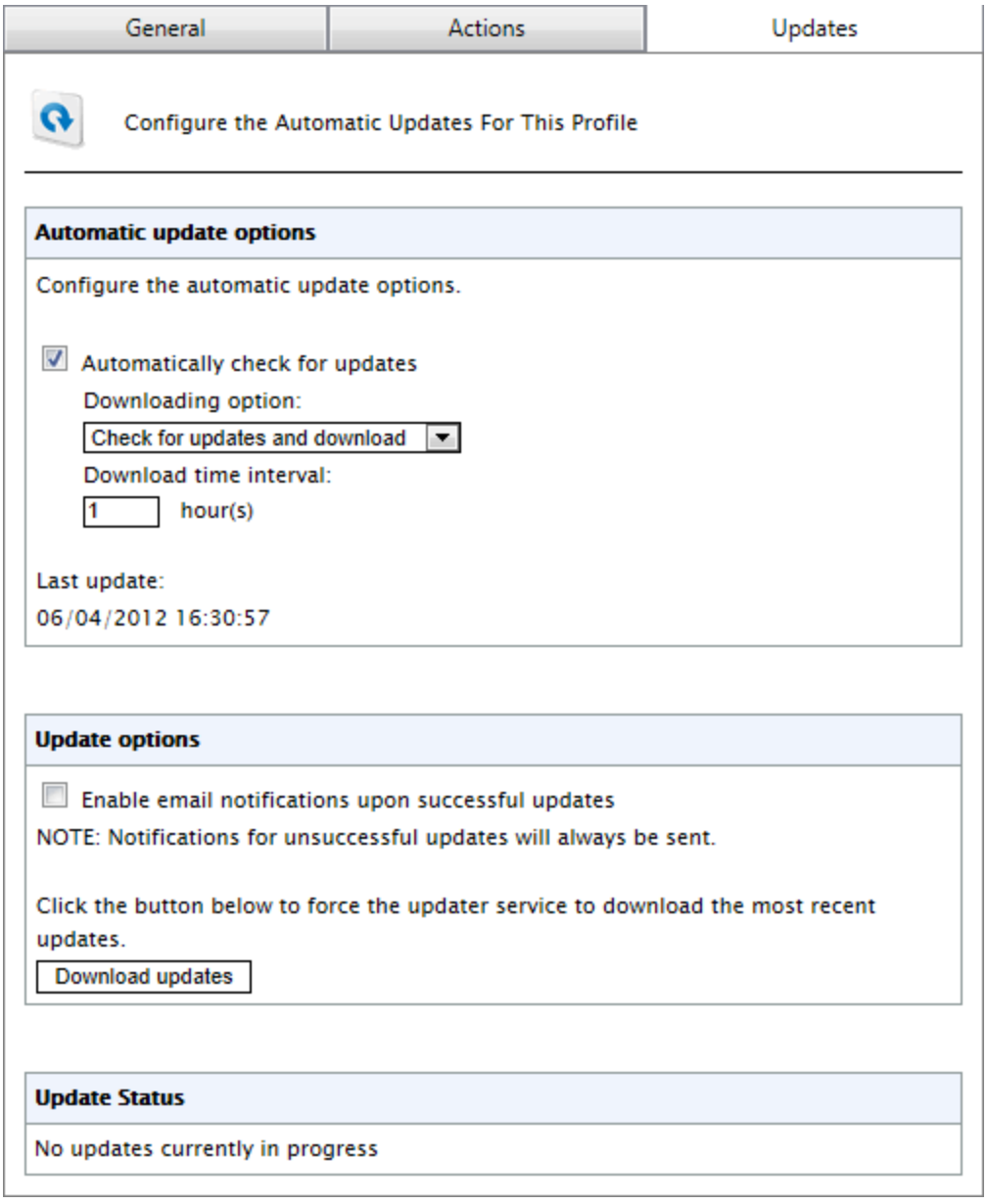
Action	Description
Quarantine email	Stores all infected emails detected by the selected Virus Scanning Engine in the Quarantine Store. You can subsequently review (approve/delete) all the quarantined emails. For more information, refer to Quarantine (page 180).
Delete email	Deletes infected emails.
Send a sanitized copy of the original email to recipient(s)	Choose whether to send a sanitized copy of the blocked email to the recipients.

6. GFI MailEssentials can send email notifications whenever an email triggers this filter. To enable this feature, select any of the following options:

Option	Description
Notify administrator	Notify the administrator whenever this engine blocks an email. For more information, refer to Administrator email address (page 219).
Notify local user	Notify the email local recipients about the blocked email.

7. To log the activity of this engine to a log file select **Log occurrence to this file**. In the text box specify path and file name to a custom location on disk where to store the log file. By default, log files are stored in:

```
<GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\Logs\<EngineName>.log
```



Screenshot 37: Virus scanning engine updates

8. From **Updates** tab, select **Automatically check for updates** to enable automatic updating of the AV files for the selected engine.

9. From **Downloading option** list, select one of the following options:

Option	Description
Only check for updates	Select this option if you want GFI MailEssentials to just check for and notify the administrator when updates are available for this engine. This option will NOT download the available updates automatically.
Check for updates and download	Select this option if you want GFI MailEssentials to check for and automatically download any updates available for this engine.

10. Specify how often you want GFI MailEssentials to check/download updates for this engine, by specifying an interval value in hours.

11. From **Update options** area, select **Enable email notifications upon successful updates** to send an email notification to the administrator whenever the engine updates successfully.

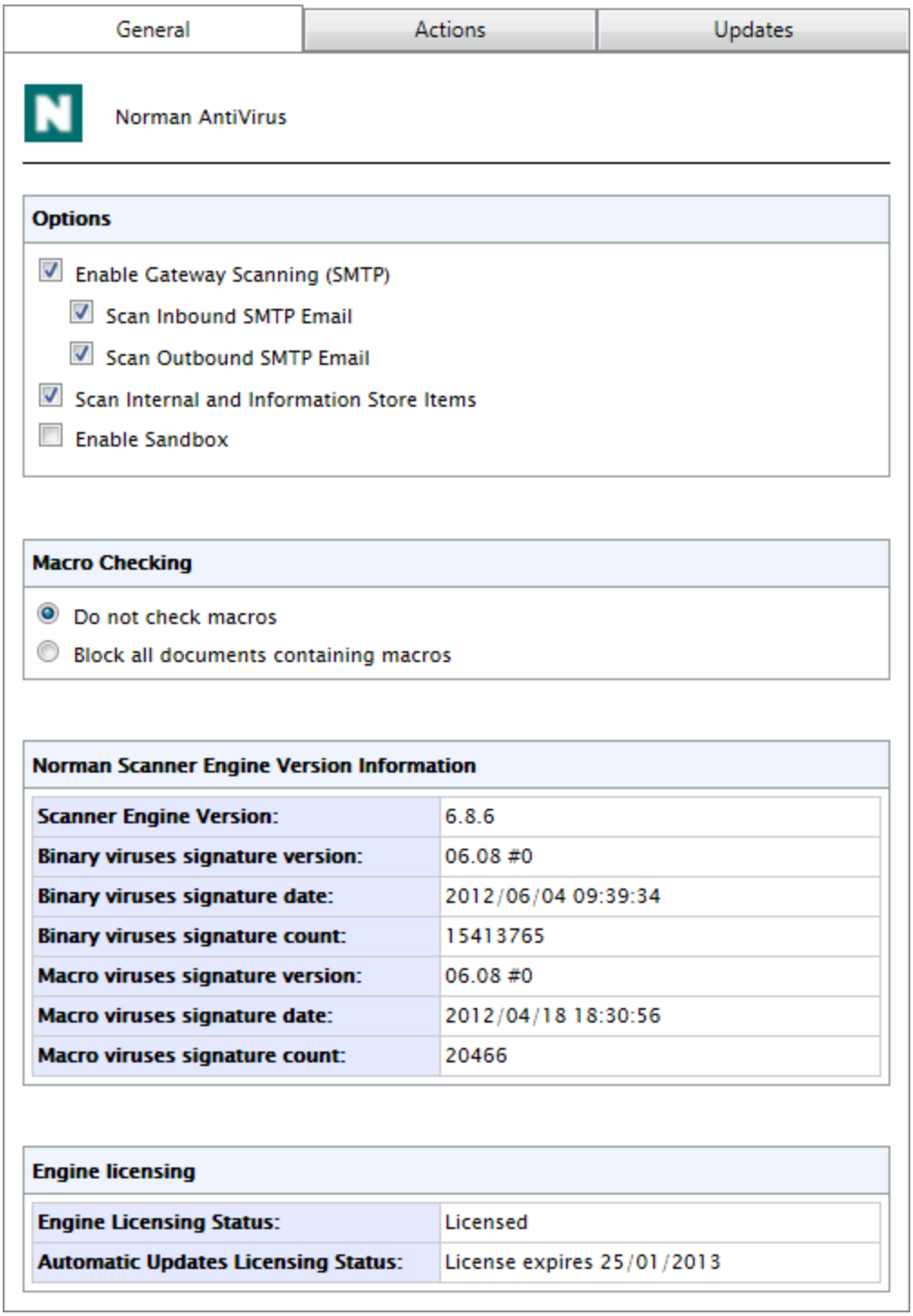
> **NOTE**
>
> An email notification is always sent when an update fails.

12. To check for and download updates immediately, click **Download updates**.

13. Click **Apply**.

6.1.4 Norman

1. Go to **Email Security > Virus Scanning Engines > Norman**.



Screenshot 38: Norman configuration

2. Select **Enable Gateway Scanning (SMTP)** check box, to scan emails using this Virus Scanning Engine.

3. Select whether to scan inbound and/or outbound emails using this Virus Scanning Engine.

Option	Description
Scan inbound SMTP email	Select this option to scan incoming emails
Scan outbound SMTP email	Select this option to scan outgoing emails

4. If you installed GFI MailEssentials on a Microsoft® Exchange machine, you will also have the option to scan internal emails and the Information Store. Select **Scan Internal and Information**

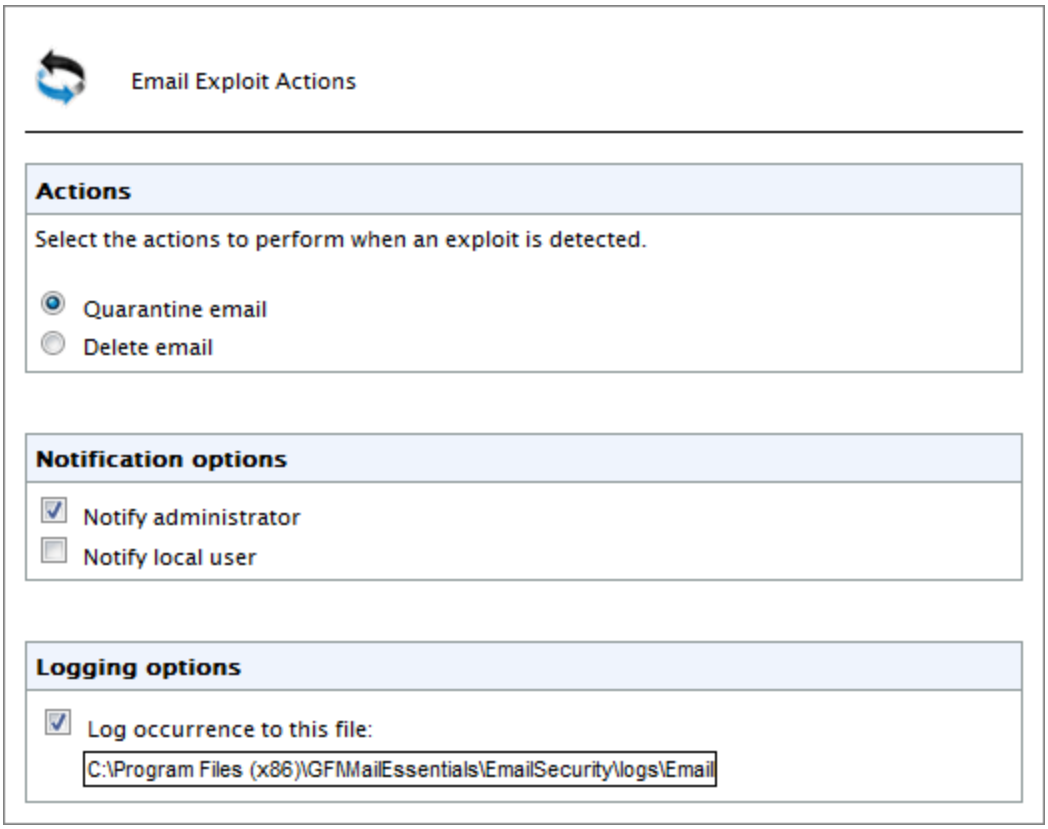
Store Items.

> **NOTE**
>
> To use the Information Store Virus Scanning feature, you must enable the option from **Information Store Protection** node. For more information, refer to Information Store Protection (page 88).

> **NOTE**
>
> In this page you can also review the antivirus engine licensing and version information.

5. Select **Enable Sandbox** to use the Norman Antivirus Sandbox feature. This executes email attachments in a virtual environment and monitors all actions and effects on a system. If an attachment exhibits viral behavior, email is marked as malicious and all appropriate actions are taken.

> **NOTE**
>
> Since this check is executed in a controlled virtual environment, it does not pose any threats to the machine or network where GFI MailEssentials is installed.



Screenshot 39: Virus scanning engine actions

6. From **Actions** tab, choose the action to take when an email is blocked:

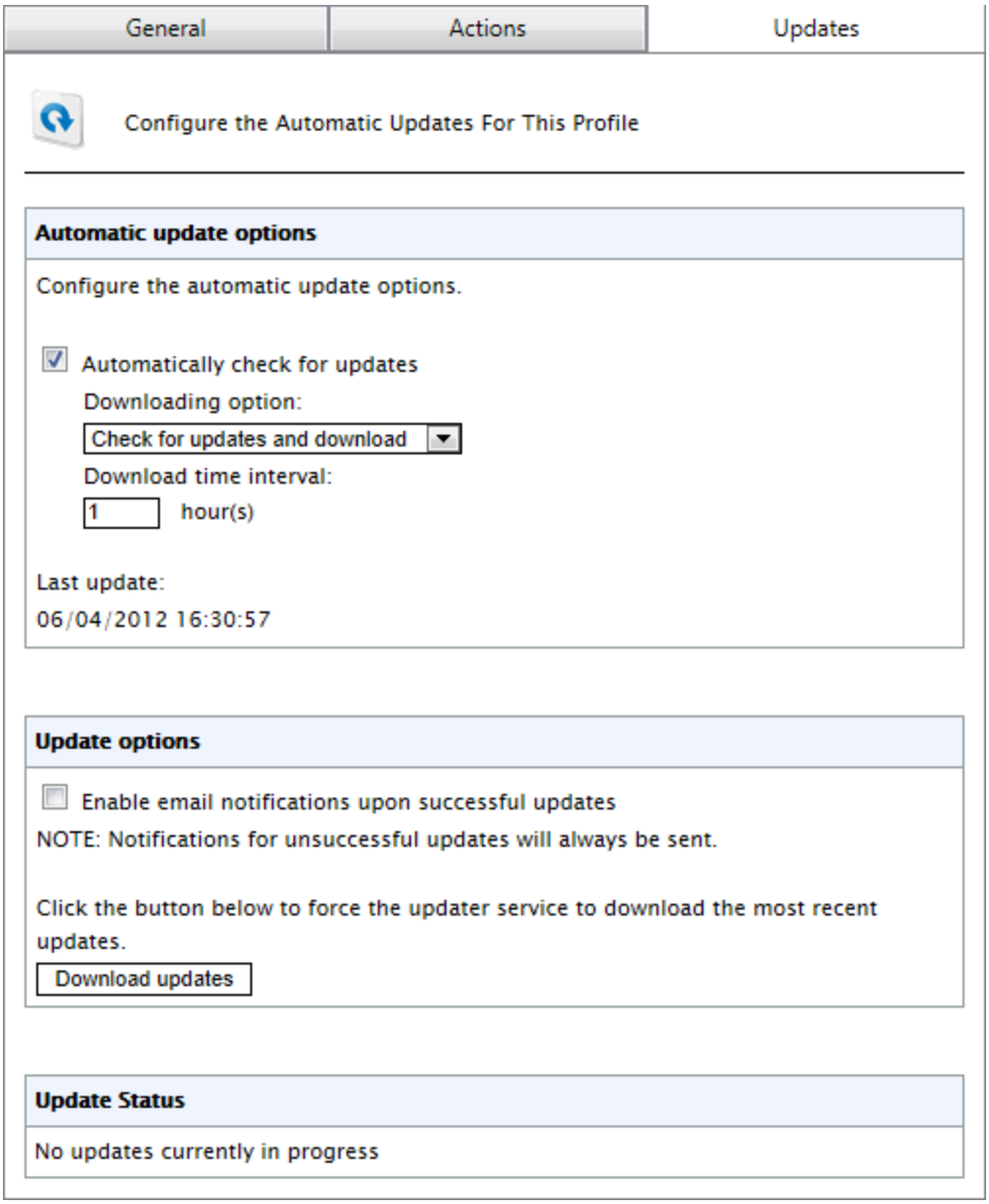
Action	Description
Quarantine email	Stores all infected emails detected by the selected Virus Scanning Engine in the Quarantine Store. You can subsequently review (approve/delete) all the quarantined emails. For more information, refer to Quarantine (page 180).
Delete email	Deletes infected emails.
Send a sanitized copy of the original email to recipient(s)	Choose whether to send a sanitized copy of the blocked email to the recipients.

7. GFI MailEssentials can send email notifications whenever an email triggers this filter. To enable this feature, select any of the following options:

Option	Description
Notify administrator	Notify the administrator whenever this engine blocks an email. For more information, refer to Administrator email address (page 219).
Notify local user	Notify the email local recipients about the blocked email.

8. To log the activity of this engine to a log file select **Log occurrence to this file**. In the text box specify path and file name to a custom location on disk where to store the log file. By default, log files are stored in:

```
<GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\Logs\<EngineName>.log
```



Screenshot 40: Virus scanning engine updates

9. From **Updates** tab, select **Automatically check for updates** to enable automatic updating of the AV files for the selected engine.

10. From **Downloading option** list, select one of the following options:

Option	Description
Only check for updates	Select this option if you want GFI MailEssentials to just check for and notify the administrator when updates are available for this engine. This option will NOT download the available updates automatically.
Check for updates and download	Select this option if you want GFI MailEssentials to check for and automatically download any updates available for this engine.

11. Specify how often you want GFI MailEssentials to check/download updates for this engine, by specifying an interval value in hours.

12. From **Update options** area, select **Enable email notifications upon successful updates** to send an email notification to the administrator whenever the engine updates successfully.

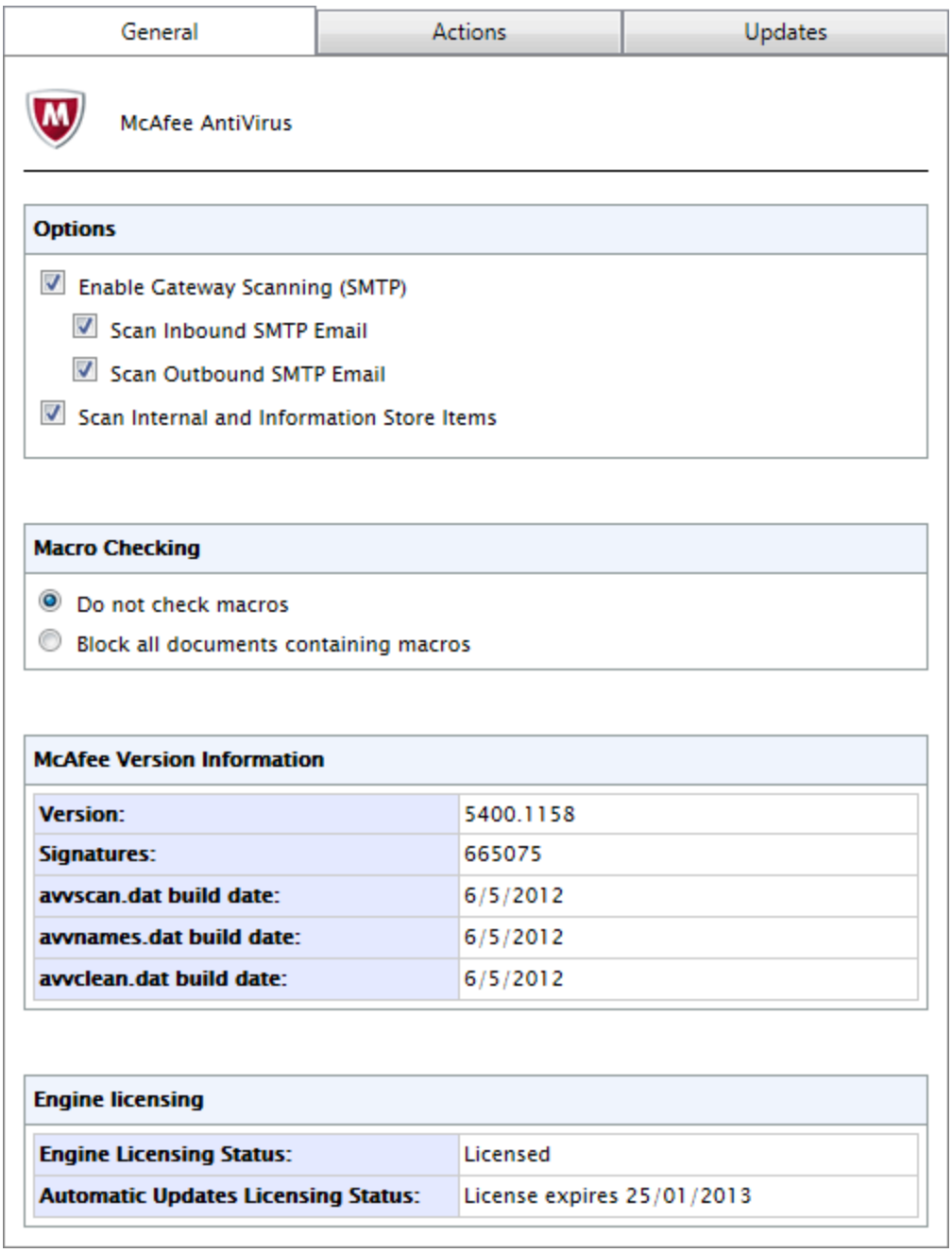
NOTE

An email notification is always sent when an update fails.

13. To check for and download updates immediately, click **Download updates**.
14. Click **Apply**.

6.1.5 McAfee

1. Go to **Email Security > Virus Scanning Engines > McAfee**.



Screenshot 41: McAfee configuration

2. Select **Enable Gateway Scanning (SMTP)** check box, to scan emails using this Virus Scanning Engine.

3. Select whether to scan inbound and/or outbound emails using this Virus Scanning Engine.

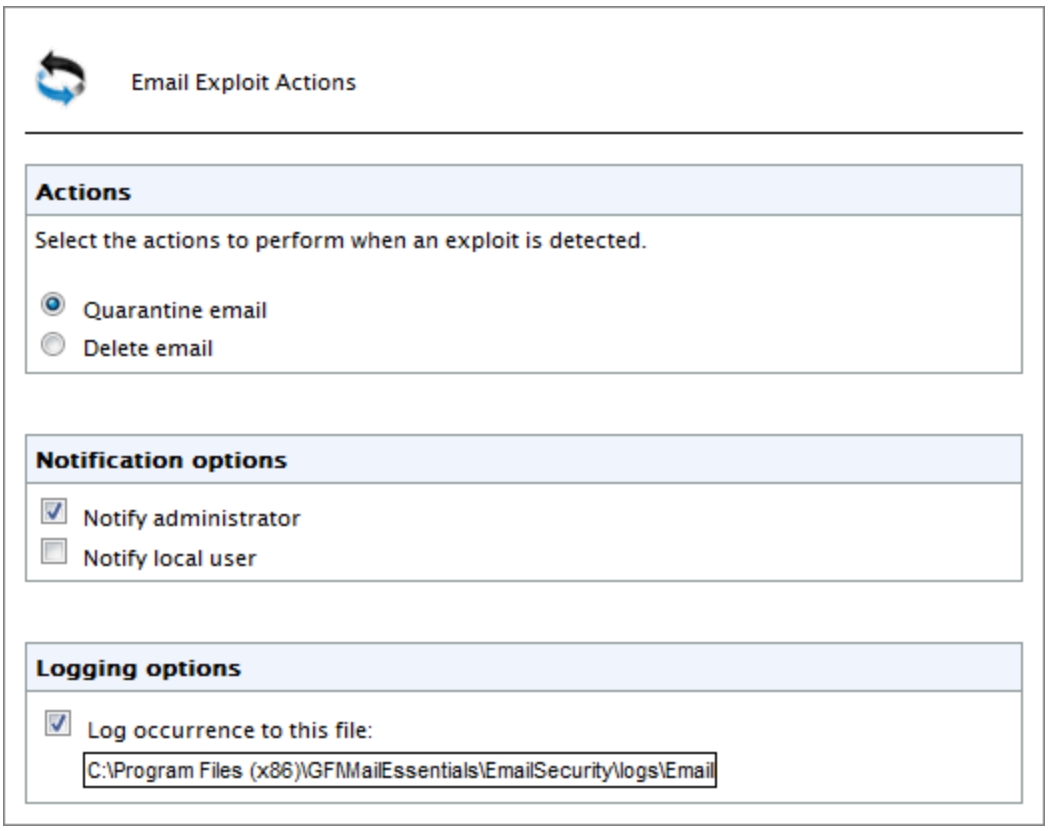
Option	Description
Scan inbound SMTP email	Select this option to scan incoming emails
Scan outbound SMTP email	Select this option to scan outgoing emails

4. If you installed GFI MailEssentials on a Microsoft® Exchange machine, you will also have the option to scan internal emails and the Information Store. Select **Scan Internal and Information Store Items**.

> **NOTE**
>
> To use the Information Store Virus Scanning feature, you must enable the option from **Information Store Protection** node. For more information, refer to Information Store Protection (page 88).

> **NOTE**
>
> In this page you can also review the antivirus engine licensing and version information.

5. McAfee Antivirus can also be used to block emails with attachments that contain macros. Enable this feature from the **Macro Checking** area by selecting **Block all documents containing macros**.



Screenshot 42: Virus scanning engine actions

6. From **Actions** tab, choose the action to take when an email is blocked:

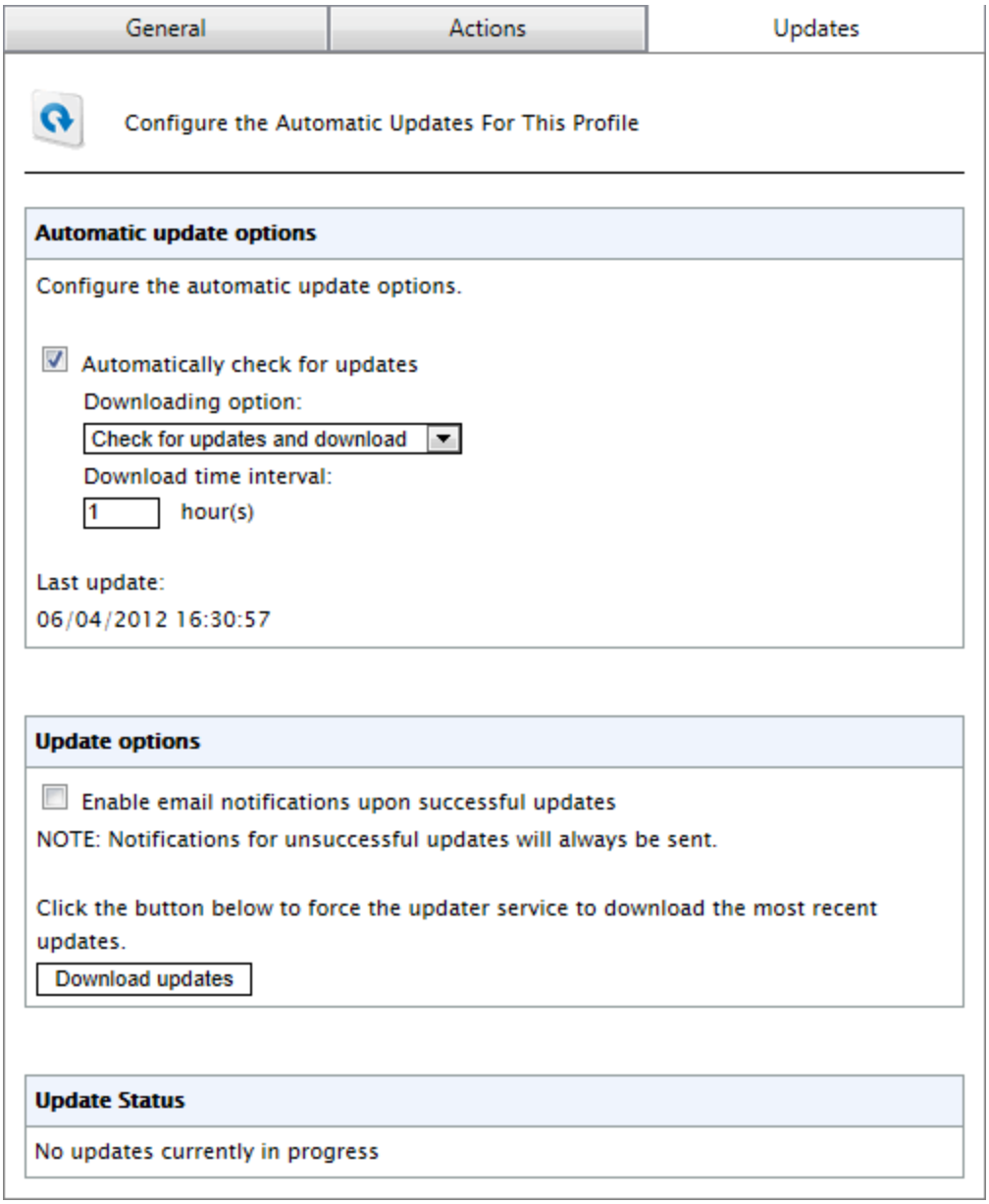
Action	Description
Quarantine email	Stores all infected emails detected by the selected Virus Scanning Engine in the Quarantine Store. You can subsequently review (approve/delete) all the quarantined emails. For more information, refer to Quarantine (page 180).
Delete email	Deletes infected emails.
Send a sanitized copy of the original email to recipient(s)	Choose whether to send a sanitized copy of the blocked email to the recipients.

7. GFI MailEssentials can send email notifications whenever an email triggers this filter. To enable this feature, select any of the following options:

Option	Description
Notify administrator	Notify the administrator whenever this engine blocks an email. For more information, refer to Administrator email address (page 219).
Notify local user	Notify the email local recipients about the blocked email.

8. To log the activity of this engine to a log file select **Log occurrence to this file**. In the text box specify path and file name to a custom location on disk where to store the log file. By default, log files are stored in:

```
<GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\Logs\<EngineName>.log
```



Screenshot 43: Virus scanning engine updates

9. From **Updates** tab, select **Automatically check for updates** to enable automatic updating of the AV files for the selected engine.

10. From **Downloading option** list, select one of the following options:

Option	Description
Only check for updates	Select this option if you want GFI MailEssentials to just check for and notify the administrator when updates are available for this engine. This option will NOT download the available updates automatically.
Check for updates and download	Select this option if you want GFI MailEssentials to check for and automatically download any updates available for this engine.

11. Specify how often you want GFI MailEssentials to check/download updates for this engine, by specifying an interval value in hours.

12. From **Update options** area, select **Enable email notifications upon successful updates** to send an email notification to the administrator whenever the engine updates successfully.

NOTE

An email notification is always sent when an update fails.

13. To check for and download updates immediately, click **Download updates**.
14. Click **Apply**.

6.2 Information Store Protection

When GFI MailEssentials is installed on the Microsoft® Exchange server machine, Information Store Protection allows you to use the Virus Scanning Engines to scan the Microsoft® Exchange Information Store for viruses.

NOTE

When GFI MailEssentials is installed on a Microsoft® Exchange Server 2007/2010 machine, Information Store Protection is available only when both the Mailbox Server Role and Hub Transport Server Role are installed.

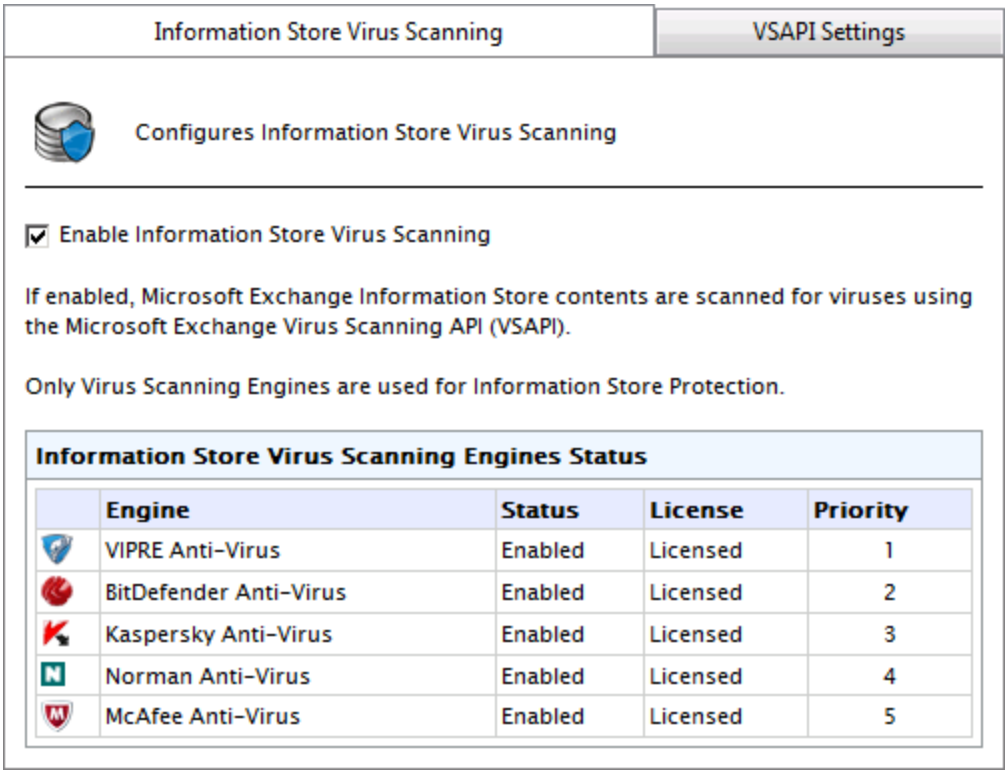
NOTE

Information Store Protection (VSAPI) is not supported on Microsoft® Exchange Server 2013 because VSAPI was removed from Microsoft® Exchange Server 2013 by Microsoft.

This section will show you how to enable Information Store Scanning and select the scan method used by VSAPI (Virus Scanning API).

6.2.1 Information Store Scanning

1. Go to **Email Security > Information Store Protection**.



Screenshot 44: Information Store Protection node

2. From **Information Store Virus Scanning** tab, select **Enable Information Store Virus Scanning**.
3. Click **Apply**.

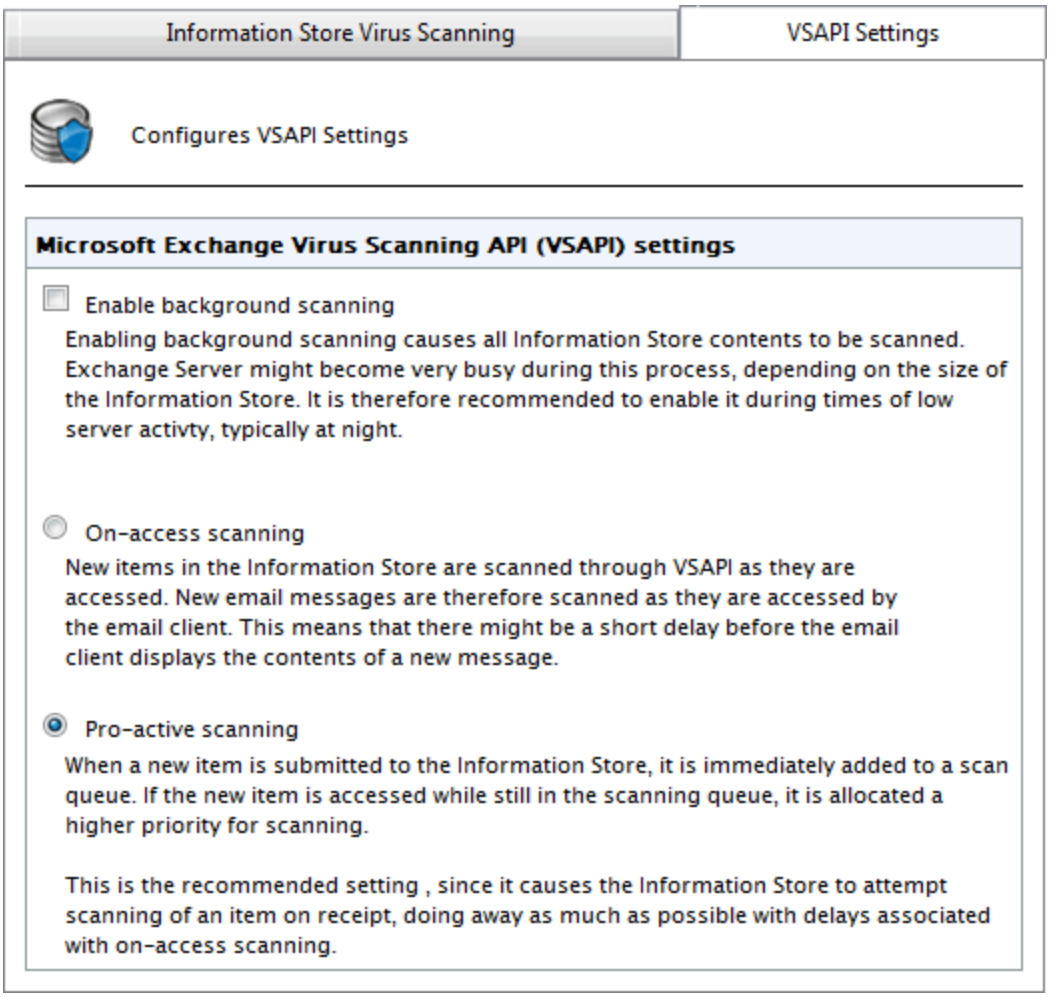
The status of the Virus Scanning Engines used to scan the Information Store is displayed in the table.

You can also disable a particular antivirus engine from Information Store Scanning. Navigate to the Virus Scanning Engines page, select the antivirus engine and disable **Scan Internal and Information Store Items**.

6.2.2 VSAPI Settings

The method used by GFI MailEssentials to access emails and attachments in the Microsoft® Exchange Information Store is VSAPI (Virus Scanning Application Programming Interface). GFI MailEssentials allows you to specify the method to use when scanning the Information Store.

1. Go to **Email Security > Information Store Protection**.
2. Select **VSAPI Settings** tab


Information Store Virus Scanning
VSAPI Settings
Configures VSAPI Settings
Microsoft Exchange Virus Scanning API (VSAPI) settings
Enable background scanning
Enabling background scanning causes all Information Store contents to be scanned. Exchange Server might become very busy during this process, depending on the size of the Information Store. It is therefore recommended to enable it during times of low server activty, typically at night.
On-access scanning
New items in the Information Store are scanned through VSAPI as they are accessed. New email messages are therefore scanned as they are accessed by the email client. This means that there might be a short delay before the email client displays the contents of a new message.
Pro-active scanning
When a new item is submitted to the Information Store, it is immediately added to a scan queue. If the new item is accessed while still in the scanning queue, it is allocated a higher priority for scanning.
This is the recommended setting , since it causes the Information Store to attempt scanning of an item on receipt, doing away as much as possible with delays associated with on-access scanning.

Screenshot 45: VSAPI Settings

3. (Optional) Select **Enable background scanning** to run Information Store Scanning in the background.

WARNING

Background scanning causes all the contents of the Information Store to be scanned. This can result in a high processing load on the Microsoft® Exchange server depending on the amount of items stored in the Information Store. It is recommended to enable this option only during periods of low server activity such as during the night.

4. Select a VSAPI scan method:

Scan Method	Description
On-access scanning	New items in the Information Store are scanned as soon as they are accessed by the email client. This introduces a short delay before the email client displays the contents of a new message.
Pro-active scanning	New items added to the Information Store are added to a queue for scanning. This is the default and recommended mode of operation, since in general the delay associated with on-access scanning is avoided. **NOTE** In the event that an email client tries to access an item that is still in the queue, it will be allocated a higher scanning priority so that it is scanned immediately.

5. Click **Apply**.

6.3 Trojan and Executable Scanner

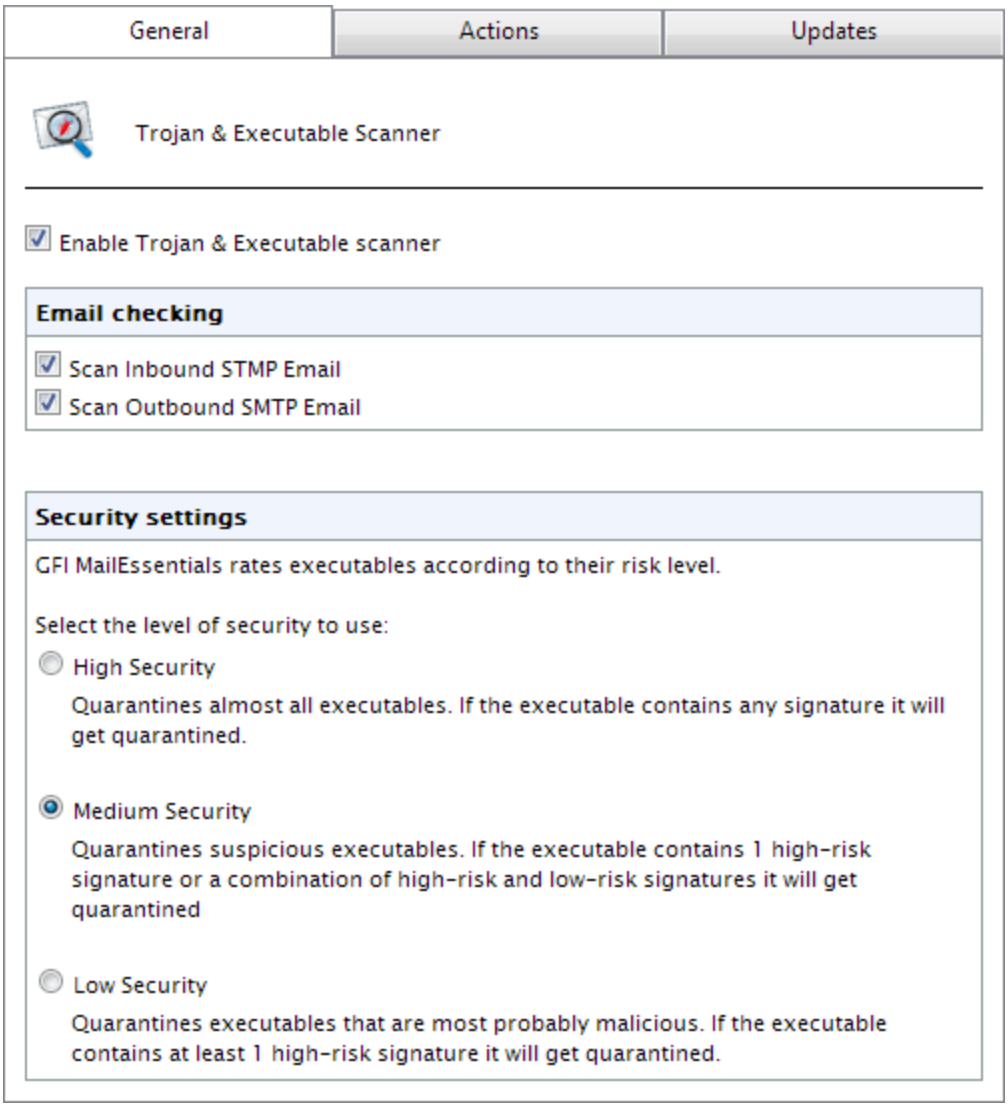
The Trojan and Executable Scanner analyzes and determines the function of executable files attached to emails. This scanner can subsequently quarantine any executables that perform suspicious activities (such as Trojans).

How does the Trojan & Executable Scanner work?

GFI MailEssentials rates the risk-level of an executable file by decompiling the executable, and detecting in real-time what the executable might do. Subsequently, it compares capabilities of the executable to a database of malicious actions and rates the risk level of the file. With the Trojan & Executable scanner, you can detect and block potentially dangerous, unknown or one-off Trojans before they compromise your network.

6.3.1 Configuring the Trojan & Executable Scanner

1. Go to **Email Security > Trojan & Executable Scanner**.


General
Actions
Updates
Trojan & Executable Scanner
Enable Trojan & Executable scanner
Email checking
Scan Inbound STMP Email
Scan Outbound SMTP Email
Security settings
GFI MailEssentials rates executables according to their risk level.
Select the level of security to use:
High Security
Quarantines almost all executables. If the executable contains any signature it will get quarantined.
Medium Security
Quarantines suspicious executables. If the executable contains 1 high-risk signature or a combination of high-risk and low-risk signatures it will get quarantined
Low Security
Quarantines executables that are most probably malicious. If the executable contains at least 1 high-risk signature it will get quarantined.

Screenshot 46: Trojan and Executable Scanner: General Tab

2. Select **Enable Trojan & Executable Scanner** to activate this filter.

3. In **Email checking** area, specify the emails to check for Trojans and other malicious executables by selecting:

Option	Description
Check inbound emails	Scan incoming emails for Trojans and malicious executable files.
Check outbound emails	Scan outgoing emails for Trojans and malicious executable files.

4. From the **Security settings** area, choose the required level of security:

Security Level	Description
High Security	Blocks all executables that contain any known malicious signatures
Medium Security	Blocks suspicious executables. Emails are blocked if an executable contains one high-risk signature or a combination of high-risk and low-risk signatures.
Low Security	Blocks only malicious executables. Emails are blocked if an executable contains at least one high-risk signature.

5. From **Actions** tab, configure the actions you want GFI MailEssentials to take on emails containing a malicious executable.

> **NOTE**
>
> Emails blocked by the Trojan & Executable Scanner are always quarantined.

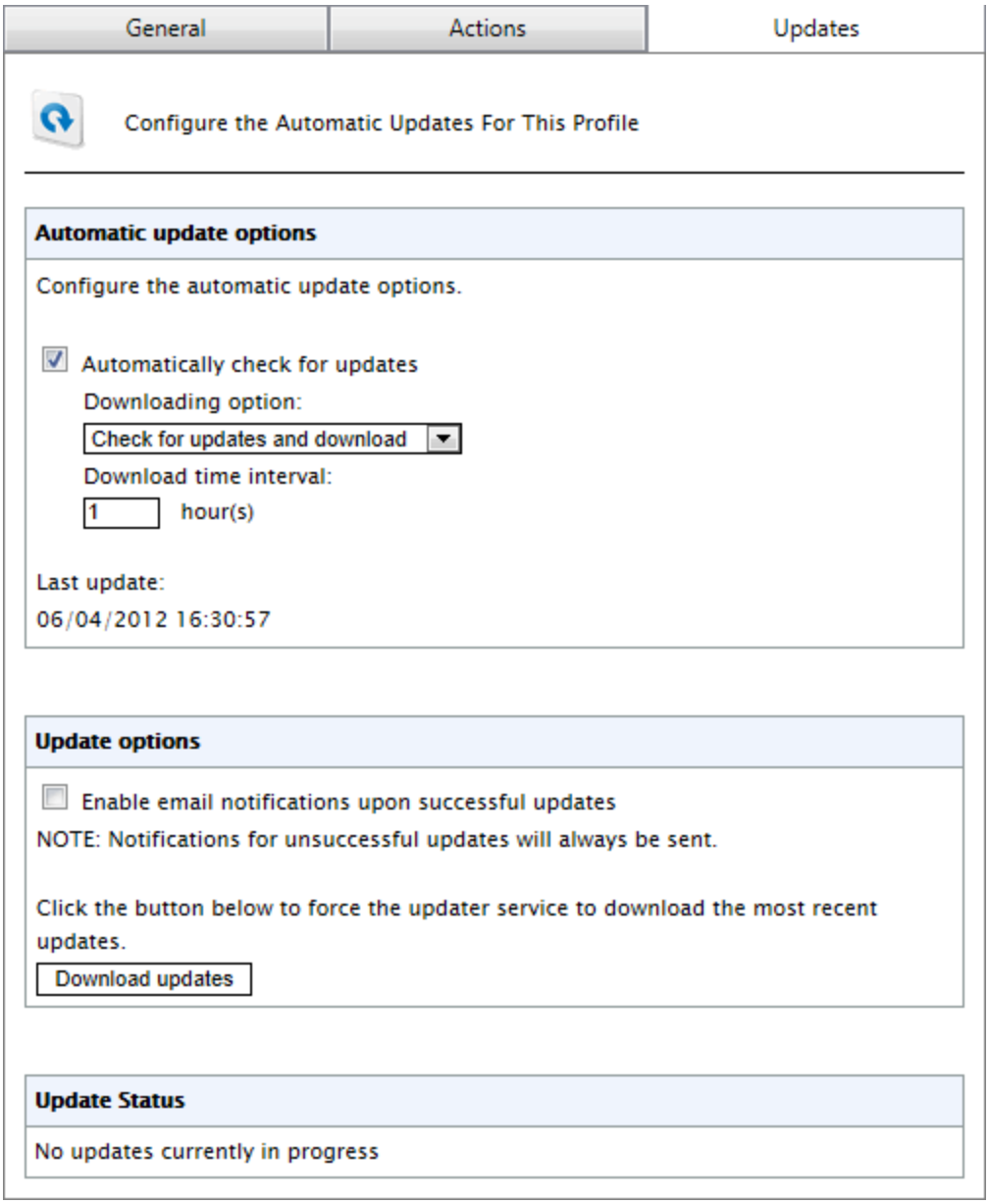
> **NOTE**
>
> When GFI MailEssentials is installed on same machine as Microsoft® Exchange 2003, GFI MailEssentials may not be able to block outbound emails, but instead replaces the blocked content with a threat report.

6. GFI MailEssentials can send email notifications whenever an email triggers this filter. To enable this feature, select any of the following options:

Option	Description
Notify administrator	Notify the administrator whenever this engine blocks an email. For more information, refer to Administrator email address (page 219).
Notify local user	Notify the email local recipients about the blocked email.

7. To log the activity of this engine to a log file select **Log occurrence to this file**. In the text box specify path and file name to a custom location on disk where to store the log file. By default, log files are stored in:

```
<GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\Logs\<EngineName>.log
```



Screenshot 47: Virus scanning engine updates

8. From **Updates** tab, select **Automatically check for updates** to enable automatic updating of the AV files for the selected engine.
9. From **Downloading option** list, select one of the following options:

Option	Description
Only check for updates	Select this option if you want GFI MailEssentials to just check for and notify the administrator when updates are available for this engine. This option will NOT download the available updates automatically.
Check for updates and download	Select this option if you want GFI MailEssentials to check for and automatically download any updates available for this engine.

10. Specify how often you want GFI MailEssentials to check/download updates for this engine, by specifying an interval value in hours.
11. From **Update options** area, select **Enable email notifications upon successful updates** to send an email notification to the administrator whenever the engine updates successfully.

NOTE

An email notification is always sent when an update fails.

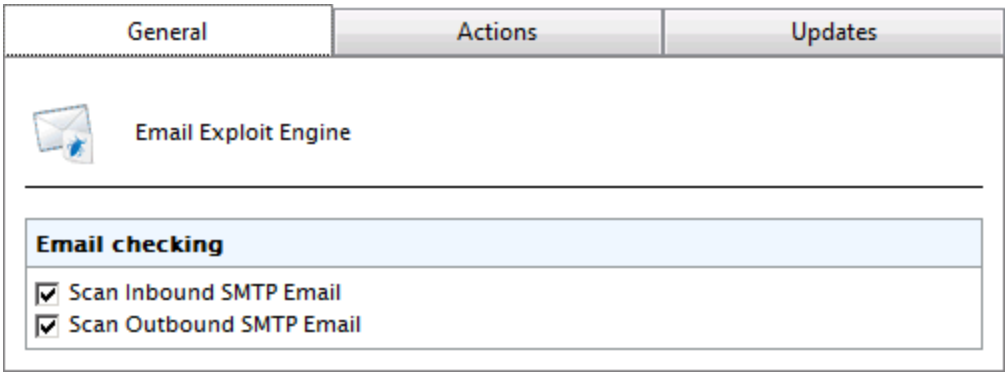
12. To check for and download updates immediately, click **Download updates**.
13. Click **Apply**.

6.4 Email Exploit Engine

The Email Exploit Engine blocks exploits embedded in an email that can execute on the recipient's machine either when the user receives or opens the email. An exploit uses known vulnerabilities in applications or operating systems to compromise the security of a system. For example, execute a program or command, or install a backdoor.

6.4.1 Configuring the Email Exploit Engine

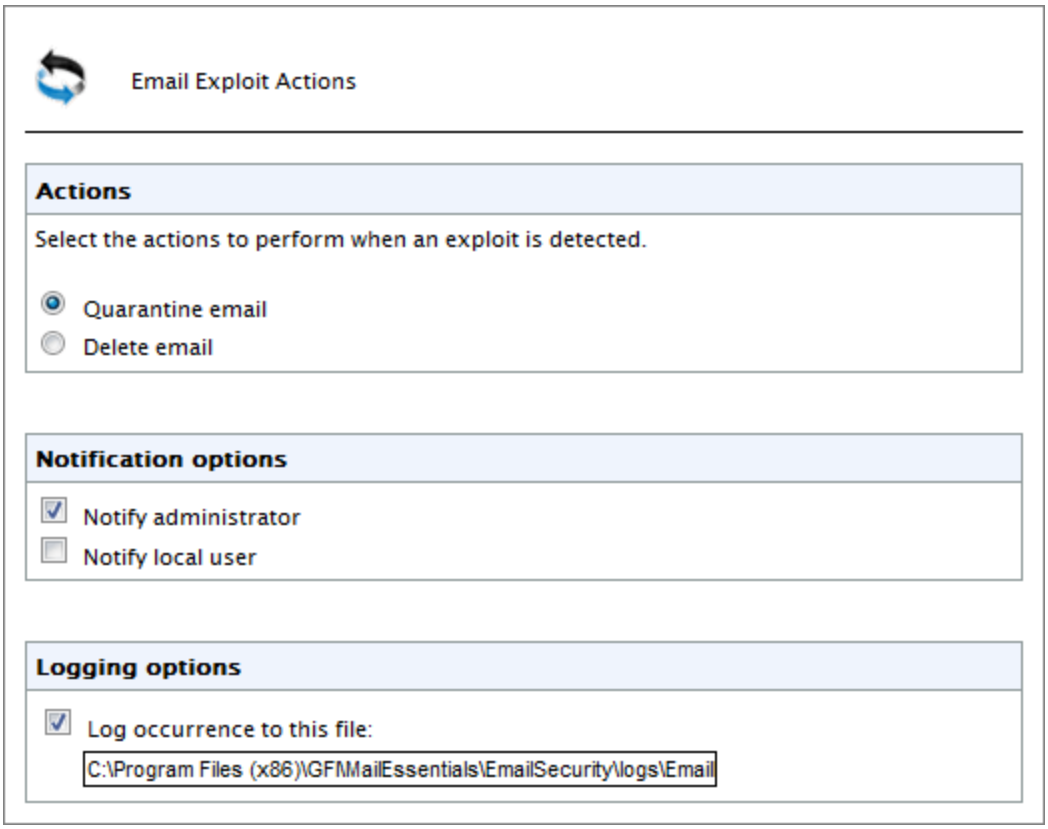
1. Go to **Email Security > Email Exploit Engine**.



Screenshot 48: Email Exploit configuration

2. From the **General** tab, select whether to scan inbound and/or outbound emails.

Option	Description
Check inbound emails	Select this option to scan incoming emails
Check outbound emails	Select this option to scan outgoing emails



Screenshot 49: Virus Scanning Engine: Configuration page (Actions Tab)

3. From **Actions** tab, choose the action to take when an email is blocked:

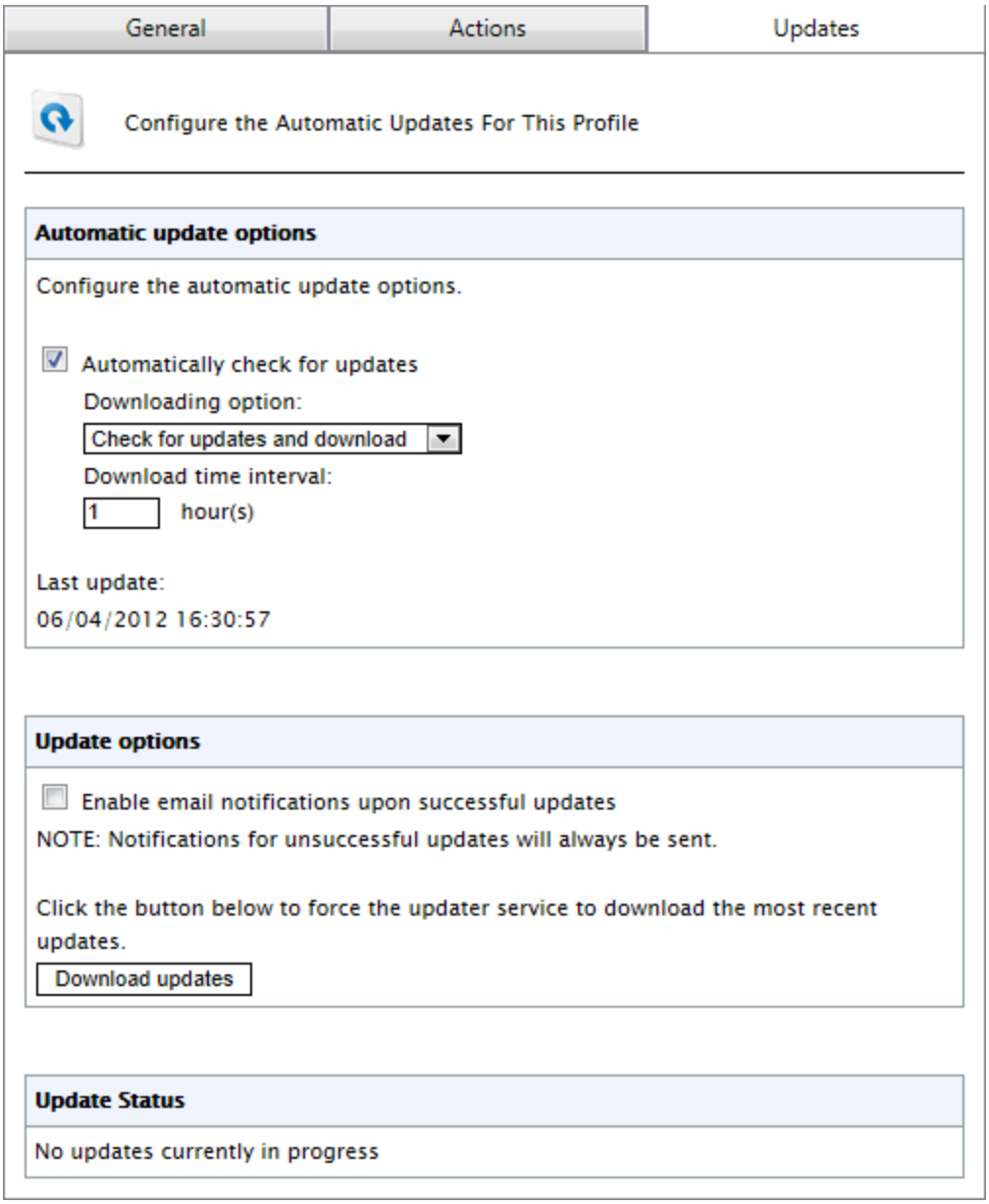
Action	Description
Quarantine item	Stores all infected emails detected by the selected Virus Scanning Engine in the Quarantine Store. You can subsequently review (approve/delete) all the quarantined emails. For more information, refer to Working with Quarantined emails (page 187).
Delete item	Deletes infected emails.

4. GFI MailEssentials can send email notifications whenever an email triggers this filter. To enable this feature, select any of the following options:

Option	Description
Notify administrator	Notify the administrator whenever this engine blocks an email. For more information, refer to Administrator email address (page 219).
Notify local user	Notify the email local recipients about the blocked email.

5. To log the activity of this engine to a log file select **Log occurrence to this file**. In the text box specify path and file name to a custom location on disk where to store the log file. By default, log files are stored in:

```
<GFI MailEssentials installation
path>\GFI\MailEssentials\EmailSecurity\Logs\<EngineName>.log
```



Screenshot 50: Virus scanning engine updates

6. From **Updates** tab, select **Automatically check for updates** to enable automatic updating of the AV files for the selected engine.
7. From **Downloading option** list, select one of the following options:

Option	Description
Only check for updates	Select this option if you want GFI MailEssentials to just check for and notify the administrator when updates are available for this engine. This option will NOT download the available updates automatically.
Check for updates and download	Select this option if you want GFI MailEssentials to check for and automatically download any updates available for this engine.

8. Specify how often you want GFI MailEssentials to check/download updates for this engine, by specifying an interval value in hours.
9. From **Update options** area, select **Enable email notifications upon successful updates** to send an email notification to the administrator whenever the engine updates successfully.

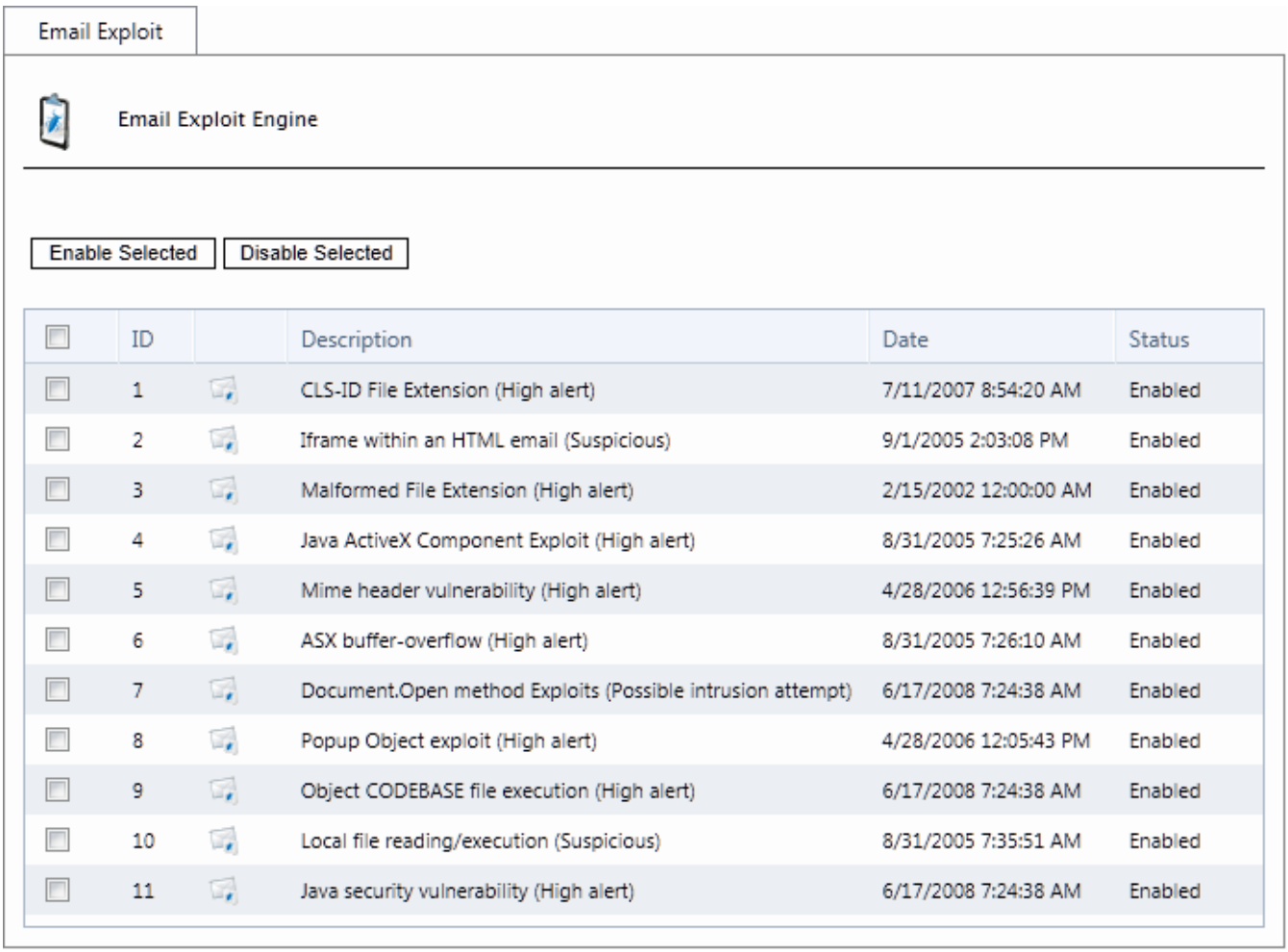
NOTE

An email notification is always sent when an update fails.

10. To check for and download updates immediately, click **Download updates**.
11. Click **Apply**.

6.4.2 Enabling/Disabling Email Exploits

1. Go to **Email Security > Email Exploit Engine > Exploit List**


Email Exploit
Email Exploit Engine
Enable Selected
Disable Selected
ID
Description
Date
Status
1 CLS-ID File Extension (High alert) 7/11/2007 8:54:20 AM Enabled
2 Iframe within an HTML email (Suspicious) 9/1/2005 2:03:08 PM Enabled
3 Malformed File Extension (High alert) 2/15/2002 12:00:00 AM Enabled
4 Java ActiveX Component Exploit (High alert) 8/31/2005 7:25:26 AM Enabled
5 Mime header vulnerability (High alert) 4/28/2006 12:56:39 PM Enabled
6 ASX buffer-overflow (High alert) 8/31/2005 7:26:10 AM Enabled
7 Document.Open method Exploits (Possible intrusion attempt) 6/17/2008 7:24:38 AM Enabled
8 Popup Object exploit (High alert) 4/28/2006 12:05:43 PM Enabled
9 Object CODEBASE file execution (High alert) 6/17/2008 7:24:38 AM Enabled
10 Local file reading/execution (Suspicious) 8/31/2005 7:35:51 AM Enabled
11 Java security vulnerability (High alert) 6/17/2008 7:24:38 AM Enabled

Screenshot 51: Email Exploit List

2. Select the check box of the exploit(s) to enable or disable.
3. Click **Enable Selected** or **Disable Selected** accordingly.

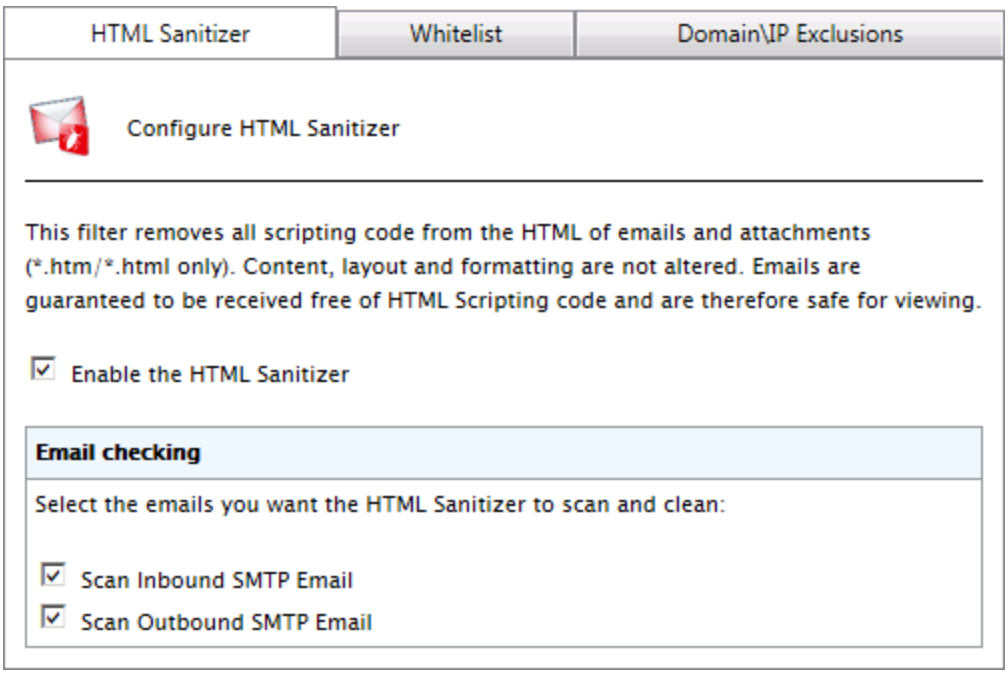
6.5 HTML Sanitizer

The HTML Sanitizer scans and removes scripting code within the email body and attachments. It scans:

- the email body of emails that have the MIME type set to “text/html”
- all attachments of type **.htm** or **.html**.

6.5.1 Configuring the HTML Sanitizer

1. Go to **Email Security > HTML Sanitizer.**


HTML Sanitizer
Whitelist
Domain\IP Exclusions
Configure HTML Sanitizer
This filter removes all scripting code from the HTML of emails and attachments (*.htm/*.html only). Content, layout and formatting are not altered. Emails are guaranteed to be received free of HTML Scripting code and are therefore safe for viewing.
Enable the HTML Sanitizer
Email checking
Select the emails you want the HTML Sanitizer to scan and clean:
Scan Inbound SMTP Email
Scan Outbound SMTP Email

Screenshot 52: HTML Sanitizer configuration page

2. Enable the HTML Sanitizer by selecting **Enable the HTML Sanitizer** checkbox .
3. Select direction of emails:

Option	Description
Check inbound emails	Scan and sanitize HTML scripts from all incoming emails.
Check outbound emails	Scan and sanitize HTML scripts from all outgoing emails.

4. Click **Apply**.

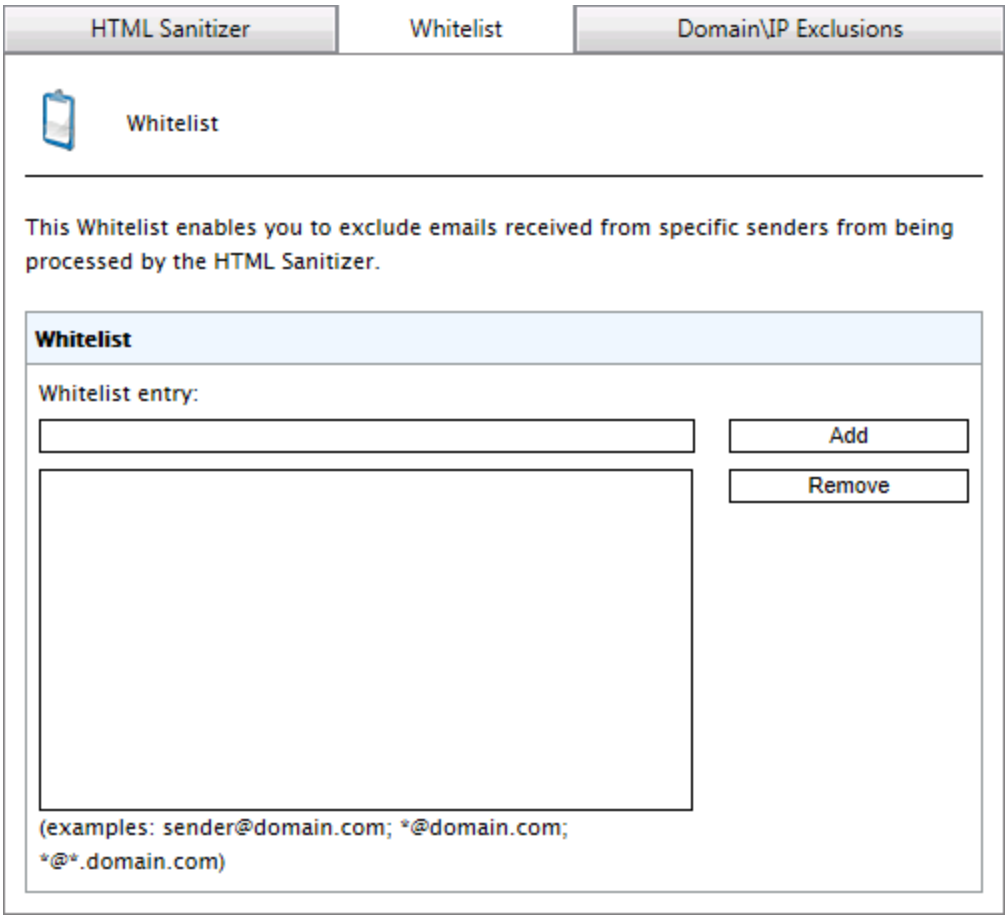
6.5.2 HTML Sanitizer Whitelist

The HTML Sanitizer Whitelist can be configured to exclude emails received from specific senders.

> **NOTE**
>
> To exclude specific IP Addresses or domains, use the HTML Santizer Domain\IP Exclusions feature. For more information, refer to HTML Sanitizer (page 97).

To manage senders in the HTML Sanitizer Whitelist:

1. Navigate to **Email Security > HTML Sanitizer** and select **Whitelist** tab.



Screenshot 53: HTML Sanitizer Whitelist page

2. In **Whitelist entry**, key in an email address, an email domain (for example, *@domain.com) or an email sub-domain (for example, *@*.domain.com) and click **Add**.

> **NOTE**
>
> To remove an entry from the HTML Sanitizer whitelist, select an entry and click **Remove**.

3. Click **Apply**.

6.5.3 HTML Santizer Domain\IP Exclusions

The HTML Santizer Domain\IP Exclusions feature enables administrators to specify IP addresses or domains to exclude from HTML Sanitizer. This will not simply use an IP address list; it can also support domain addresses, which are then resolved at runtime, so that all the IP addresses for the domain in question are obtained. This is done in two ways:

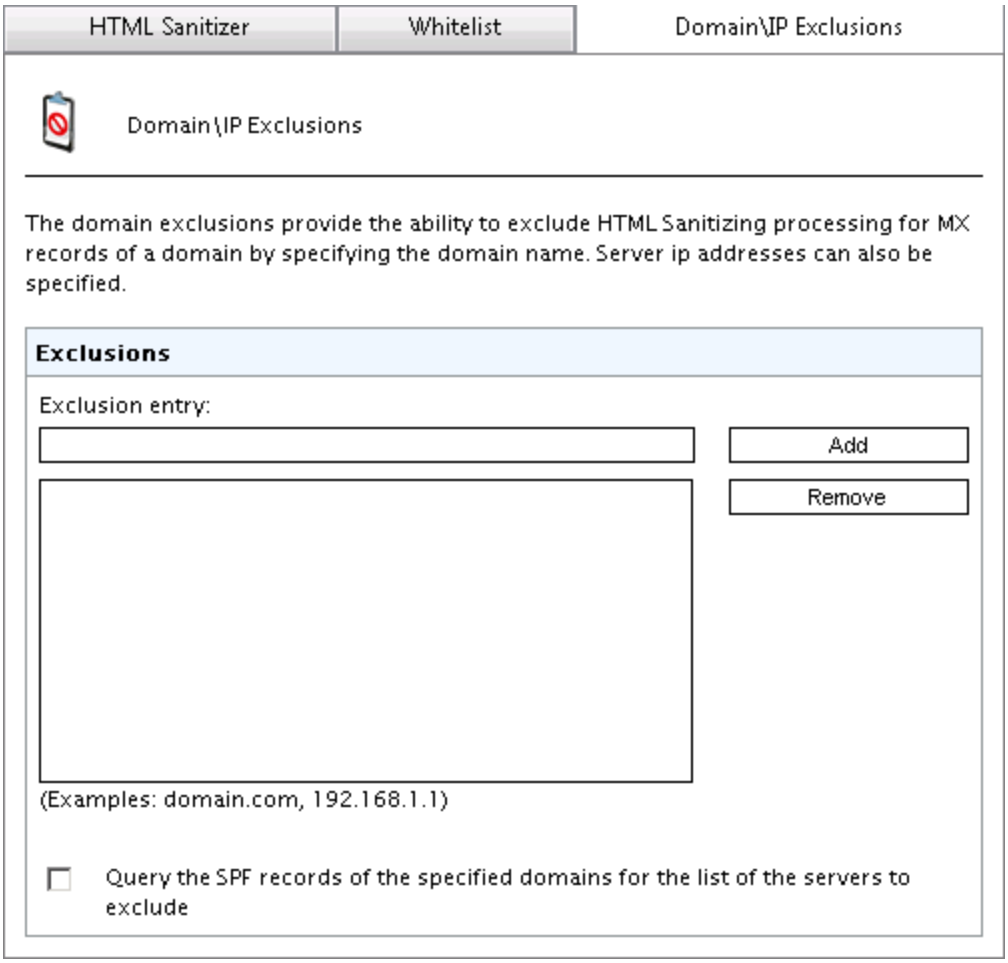
1. By default, the feature queries the MX records of the domain being processed
2. Optionally,you can choose to have the SPF record of the domain queried. If the domain doesn't have an SPF record, the SPF part is ignored and only the MX records are used.

If the IP address from where the email originated (the one which sent to the perimeter server) is an IP listed in the Domains\IPs exclusions tab or resolved from a domain in the same list, then the email is not processed by HTML Sanitizer. This is a sort of IP Whitelist but with the additional benefit of

specifying domains and have the feature resolve the domains' MX records and (optionally) the SPF record to get the IP addresses.

To manage domains\IP exclusions in the HTML Sanitizer Whitelist:

1. Navigate to **Email Security > HTML Sanitizer** and select **Domains\IP exclusions** tab.


HTML Sanitizer
Whitelist
Domain\IP Exclusions
Domain\IP Exclusions
The domain exclusions provide the ability to exclude HTML Sanitizing processing for MX records of a domain by specifying the domain name. Server ip addresses can also be specified.
Exclusions
Exclusion entry:
Add
Remove
(Examples: domain.com, 192.168.1.1)
Query the SPF records of the specified domains for the list of the servers to exclude

Screenshot 54: Domain\IP Exclusions

2. Key in the domain or IP address to exclude and click **Add**.

> **NOTE**
>
> To remove an entry from the HTML Sanitizer Domain\IP Exclusions, select an entry and click **Remove**.

3. Optionally, select **Query the SPF records of the specified domains for the list of the servers to exclude**.
4. Click **Apply**.

7 Anti-Spam

The anti-spam filters included with GFI MailEssentials help detect and block unwanted emails (spam).

Topics in this chapter:

7.1 Anti-Spam filters 101
7.1.1 SpamRazer 102
7.1.2 Anti-Phishing 105
7.1.3 Directory Harvesting 107
7.1.4 Email blocklist 110
7.1.5 IP DNS Blocklist 112
7.1.6 URI DNS Blocklist 114
7.1.7 Sender Policy Framework 115
7.1.8 Anti-Spoofing 117
7.1.9 Greylist 119
7.1.10 Header Checking 121
7.1.11 Spam Keyword Checking 124
7.1.12 Bayesian Analysis 128
7.1.13 Whitelist 130
7.1.14 New Senders 134
7.2 Spam Actions - What to do with spam emails 135
7.2.1 Configuring Spam Actions 136
7.3 Sorting anti-spam filters by priority 138
7.4 Spam Digest 139
7.4.1 Configuring spam digests - Administrator spam digest 139
7.4.2 Configuring spam digests - Recipient spam digest 140
7.5 Anti-Spam settings 142
7.5.1 Log file rotation 143
7.5.2 Anti-Spam Global Actions 143
7.5.3 DNS Server Settings 144
7.5.4 Remote Commands 145
7.5.5 Perimeter SMTP Server Settings 148
7.6 Public Folder Scanning 149
7.6.1 Enabling Public Folder Scanning 149
7.6.2 Using Public folder scanning 153

7.1 Anti-Spam filters

GFI MailEssentials uses various scanning filters to identify spam:

FILTER	DESCRIPTION	ENABLED BY DEFAULT
SpamRazer	An anti-spam engine that determines if an email is spam by using email reputation, message fingerprinting and content analysis.	Yes
Anti-Phishing	Blocks emails that contain links in the message body pointing to known phishing sites or if they contain typical phishing keywords.	Yes

FILTER	DESCRIPTION	ENABLED BY DEFAULT
Director Harvesting	Directory harvesting attacks occur when spammers try to guess email addresses by attaching well known usernames to your domain. The majority of the email addresses are non-existent.	Yes (only if GFI MailEssentials is installed in an Active Directory environment)
Email Blocklist	The Email Blocklist is a custom database of email addresses and domains from which you never want to receive emails.	Yes
IP DNS Blocklist	IP DNS Blocklist checks the IP address of the sending mail server against a public list of mail servers known to send spam.	Yes
URI DNS Blocklist	Stops emails that contain links to domains listed on public Spam URI Blocklists.	Yes
Sender Policy Framework	This filter uses SPF records to stop email sent from forged IP addresses by identifying if the sender IP address is authorized.	No
Anti-Spoofing	Checks emails received with a sender email address claiming to originate from your own domain against a list of IP addresses by GFI MailEssentials. If the sender IP address is not on the list of own-domain server IP addresses, email is blocked.	No
Greylist	The Greylist filter temporarily blocks incoming emails received from unknown senders. Legitimate mail systems typically try to send the email after a few minutes; spammers simply ignore such error messages.	No
Header Checking	The Header Checking filter analyses the email header to identify spam emails.	Yes
Spam Keyword Checking	This filter enables the identification of Spam based on keywords in the email being received.	No
Bayesian analysis	An anti-spam filter that can be trained to accurately determine if an email is spam based on past experience.	No
Whitelist	The Whitelist contains lists of criteria that identify legitimate email. Emails that match these criteria are not scanned by anti-spam filters and are always delivered to the recipient.	Yes
New Senders	The New Senders filter identifies emails that have been received from senders to whom emails have never been sent before.	No

7.1.1 SpamRazer

An anti-spam engine that determines if an email is spam by using email reputation, message fingerprinting and content analysis. SpamRazer is the primary anti-spam engine and is enabled by default on installation. Frequent updates are released for SpamRazer that will further increase the response time to new trends of spam.

SpamRazer also includes Sender Policy Framework filtering which detects forged senders. It is recommended that senders publish their mail server in an SPF record. For more information on SPF and how it works, visit the Sender Policy Framework website at: http://www.openspf.org.

This filter also blocks NDR spam. For more information on NDR spam refer to http://go.gfi.com/?pageid=ME_NDRSpam

Configuring SpamRazer

NOTE

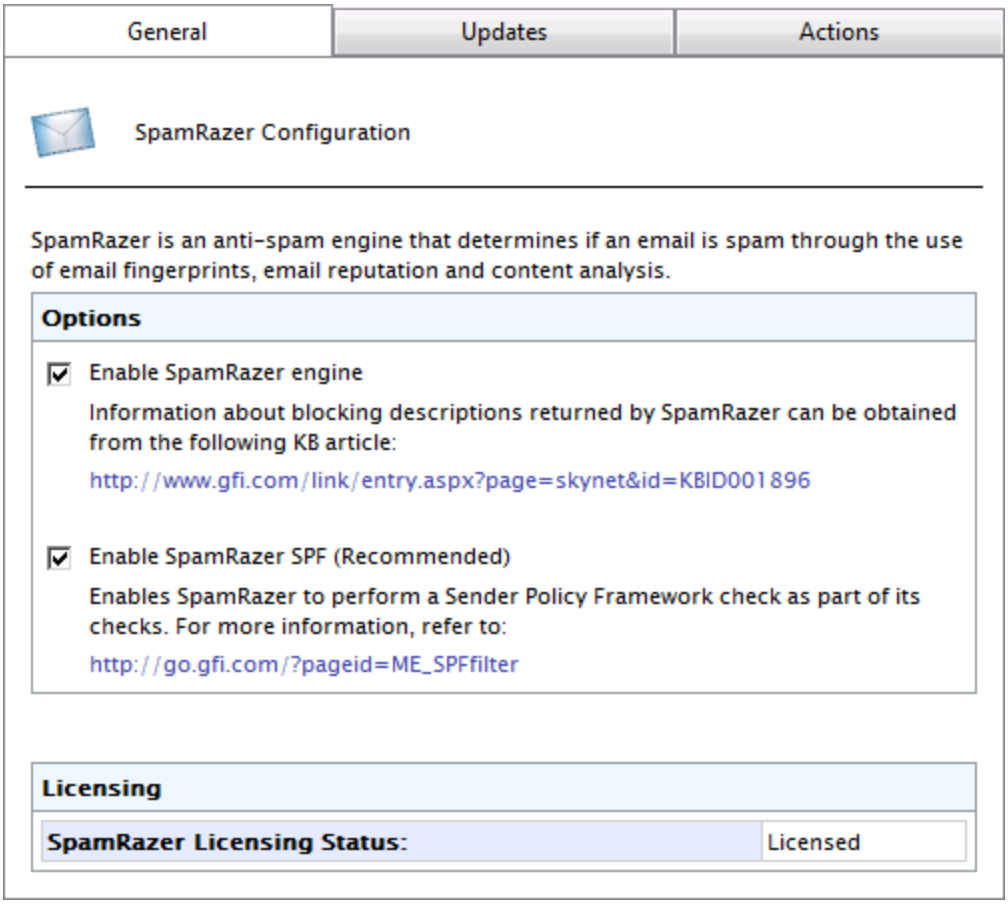
Disabling SpamRazer is **NOT** recommended.

NOTE

GFI MailEssentials downloads SpamRazer updates from:

*.mailshell.net

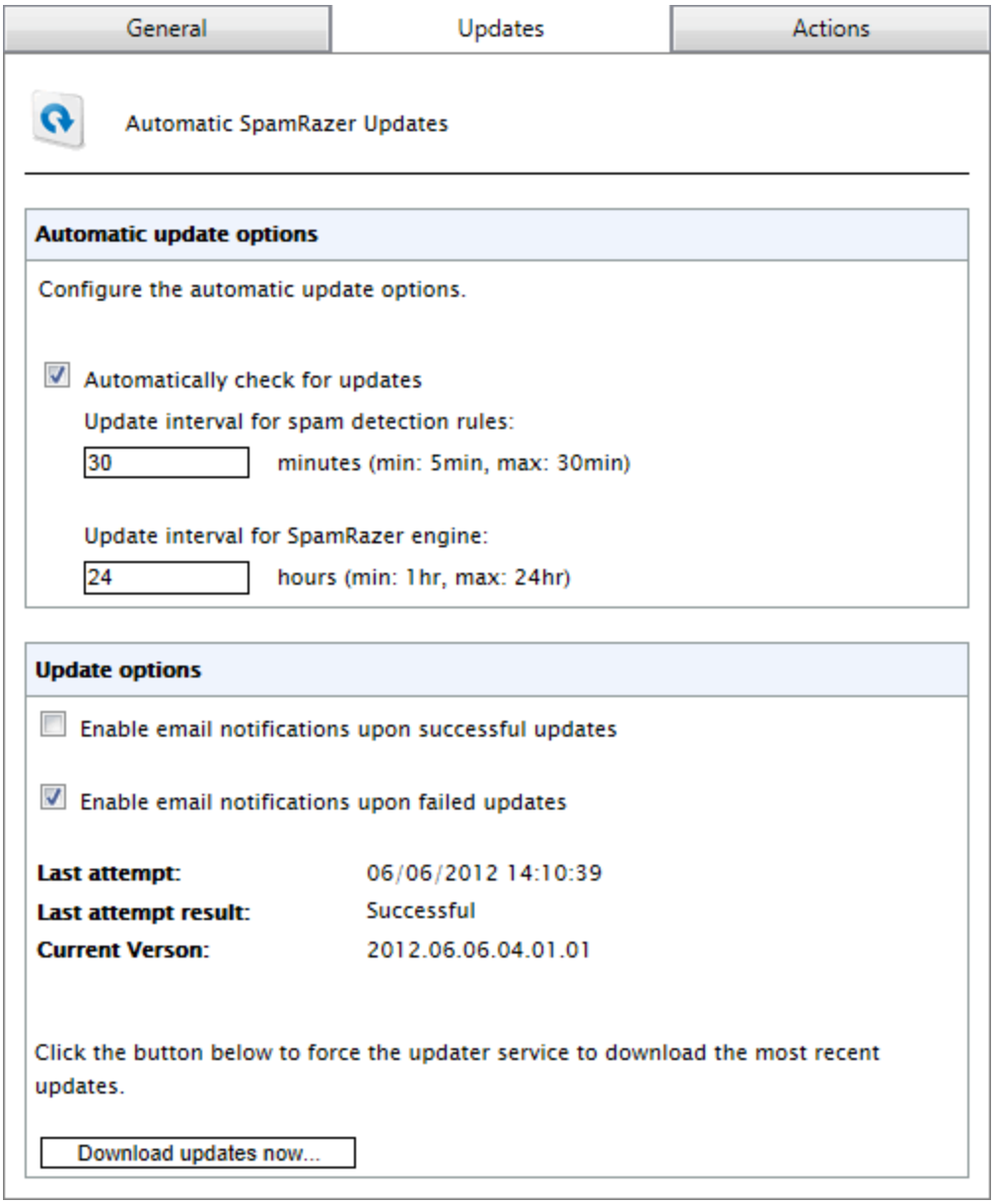
1. Go to **Anti-Spam > Anti-Spam Filters > SpamRazer**.


General
Updates
Actions
SpamRazer Configuration
SpamRazer is an anti-spam engine that determines if an email is spam through the use of email fingerprints, email reputation and content analysis.
Options
Enable SpamRazer engine
Information about blocking descriptions returned by SpamRazer can be obtained from the following KB article:
http://www.gfi.com/link/entry.aspx?page=skynet&id=KBID001896
Enable SpamRazer SPF (Recommended)
Enables SpamRazer to perform a Sender Policy Framework check as part of its checks. For more information, refer to:
http://go.gfi.com/?pageid=ME_SPFfilter
Licensing
SpamRazer Licensing Status:
Licensed

Screenshot 55: SpamRazer Properties

2. From the **General** tab perform any of the following actions:

Option	Description
Enable SpamRazer engine	Enable or disable SpamRazer.
Enable SpamRazer SPF (Recommended)	Enable or disable Sender Policy Framework. It is recommended to enable this option and to have this filter running after to the Email Whitelist.


General
Updates
Actions
Automatic SpamRazer Updates
Automatic update options
Configure the automatic update options.
Automatically check for updates
Update interval for spam detection rules:
30
minutes (min: 5min, max: 30min)
Update interval for SpamRazer engine:
24
hours (min: 1hr, max: 24hr)
Update options
Enable email notifications upon successful updates
Enable email notifications upon failed updates
Last attempt: 06/06/2012 14:10:39
Last attempt result: Successful
Current Verson: 2012.06.06.04.01.01
Click the button below to force the updater service to download the most recent updates.
Download updates now...

Screenshot 56: SpamRazer Updates tab

3. From the **Updates** tab, perform any of the following actions:

Option	Description
Automatically check for updates	Configure GFI MailEssentials to automatically check for and download any SpamRazer updates. Specify the time interval in minutes when to check for spam detection rule and SpamRazer engine updates. **NOTE** It is recommended to enable this option for SpamRazer to be more effective in detecting the latest spam trends.
Enable email notifications upon successful updates	Select this option to be informed via email when new updates are downloaded.
Enable email notifications upon failed updates	Select this option to be informed via email when a download or installation fails.
Download updates now...	Click to download updates.

NOTE

You can download updates using a proxy server. For more information, refer to Proxy settings (page 221).

4. Click **Actions** tab to select the actions to perform on messages identified as spam. For more information, refer to Spam Actions - What to do with spam emails (page 135).
5. Click **Apply**.

7.1.2 Anti-Phishing

Blocks emails that contain links in the message body pointing to known phishing sites or if they contain typical phishing keywords. Phishing is an email based social engineering technique aimed at having email users disclose personal details to spammers. A phishing email is most likely crafted to resemble an official email originating from a reputable business, for example a bank. Phishing emails will usually contain instructions requiring users to reconfirm sensitive information such as online banking details or credit card information. Phishing emails usually include a phishing Uniform Resource Identifier (URI) that the user is supposed to follow to key in some sensitive information on a phishing site. The site pointed to by the phishing URI might be a replica of an official site, but in reality it is controlled by whoever sent the phishing emails. When the user enters the sensitive information on the phishing site, the data is collected and used, for example, to withdraw money from bank accounts.

The Anti-Phishing filter detects phishing emails by comparing URIs present in the email to a database of URIs known to be used in phishing attacks. Phishing also looks for typical phishing keywords in the URIs.

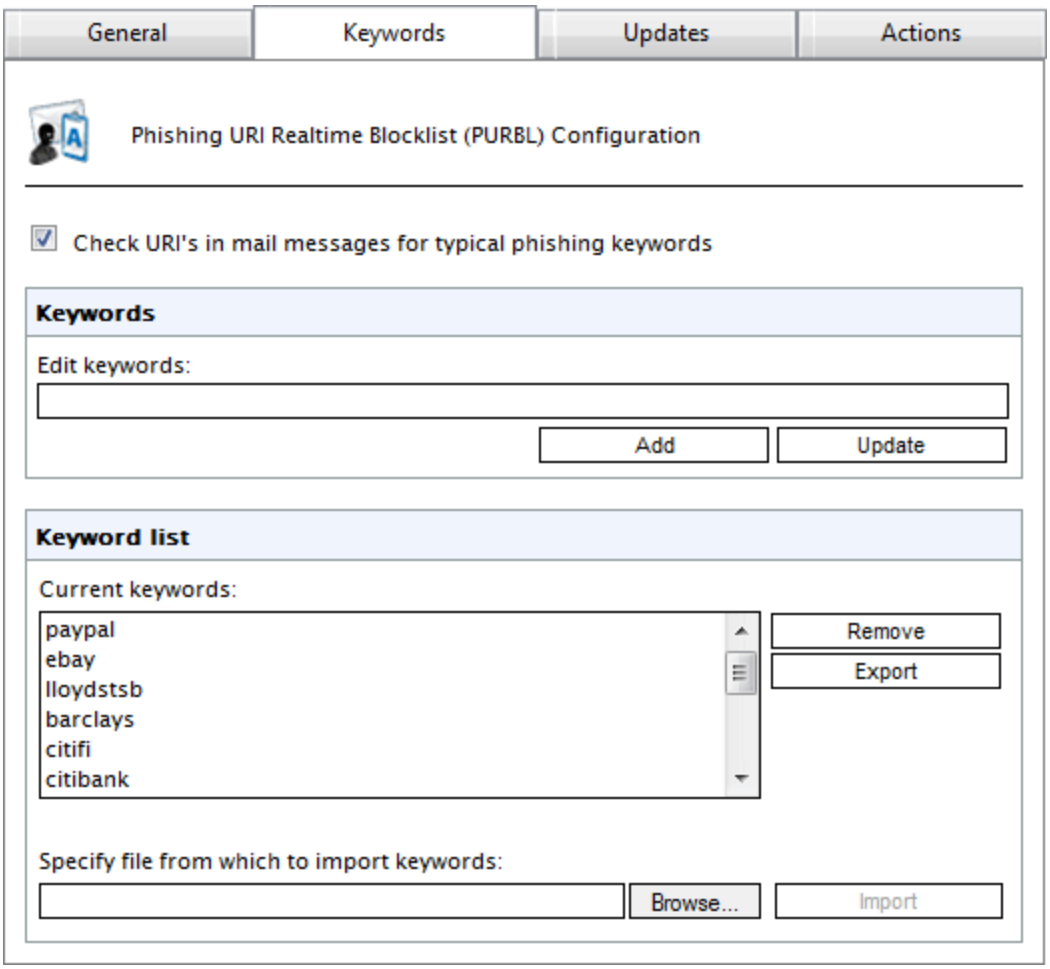
The Anti-Phishing filter is enabled by default on installation.

Configuring Anti-Phishing

NOTE

Disabling Anti-Phishing is **NOT** recommended.

1. Go to **Anti-Spam > Anti-Spam Filters > Anti-Phishing**.



Screenshot 57: Anti-Phishing options

2. From the **General** tab, select/unselect **Check mail messages for URI's to known phishing sites** option to enable/disable Anti-Phishing.

3. From the **Keywords** tab select any of the following options:

Option	Description
Check URI's in mail messages for typical phishing keywords	Enable/disable checks for typical phishing keywords
Add	Enables adding keywords to Phishing filter. Key in a keyword and click **Add** to add a keyword to the Anti-Phishing filter
Update	Enables updating selected keywords. Select a keyword from the **Current Keywords** list, make any changes to keyword in **Edit Keywords** field and click **Update**.
Remove	Enables removing selected keywords from list. Select a keyword from the **Current Keywords** list, and click **Remove**.
Export	Exports current list to an XML format file.
Browse...	Enables importing of a previously exported keyword list. Click **Browse**, select a previously exported keyword file and click **Import**.

4. From the **Updates** tab, select any of the following options:

Option	Description
Automatically check for updates	Configure GFI MailEssentials to automatically check for and download any Anti-Phishing updates. Specify the time interval in minutes when to check for updates. **NOTE** It is recommended to enable this option for Anti-Phishing to be more effective in detecting the latest phishing trends.
Enable email notifications upon successful updates	Select/unselect checkbox to be informed via email when new updates are downloaded.
Enable email notifications upon failed updates	Select/unselect to be informed when a download or installation fails.
Download updates now	Click to immediately download Anti-Phishing updates.

NOTE

You can download updates using a proxy server. For more information, refer to Proxy settings (page 221).

5. Click **Actions** tab to select the actions to perform on messages identified as spam. For more information, refer to Spam Actions - What to do with spam emails (page 135).
6. Click **Apply**.

7.1.3 Directory Harvesting

Directory harvesting attacks occur when spammers try to guess email addresses by attaching well known usernames to your domain. The majority of the email addresses are non-existent.Spammers send emails to randomly generated email addresses and while some email addresses may match real users, the majority of these messages are invalid and consequently floods the victim's email server.

GFI MailEssentials stops these attacks by blocking emails addressed to users not in the organizations' Active Directory or email server.

Directory harvesting can either be configured to execute when the full email is received or at SMTP level, that is, emails are filtered while they are being received. SMTP level filtering terminates the email's connection and therefore stops the download of the full email, economizing on bandwidth and processing resources. In this case the connection is terminated immediately and emails are not required to go through any other anti-spam filters.

This filter is enabled by default on installing GFI MailEssentials in an Active Directory Environment.

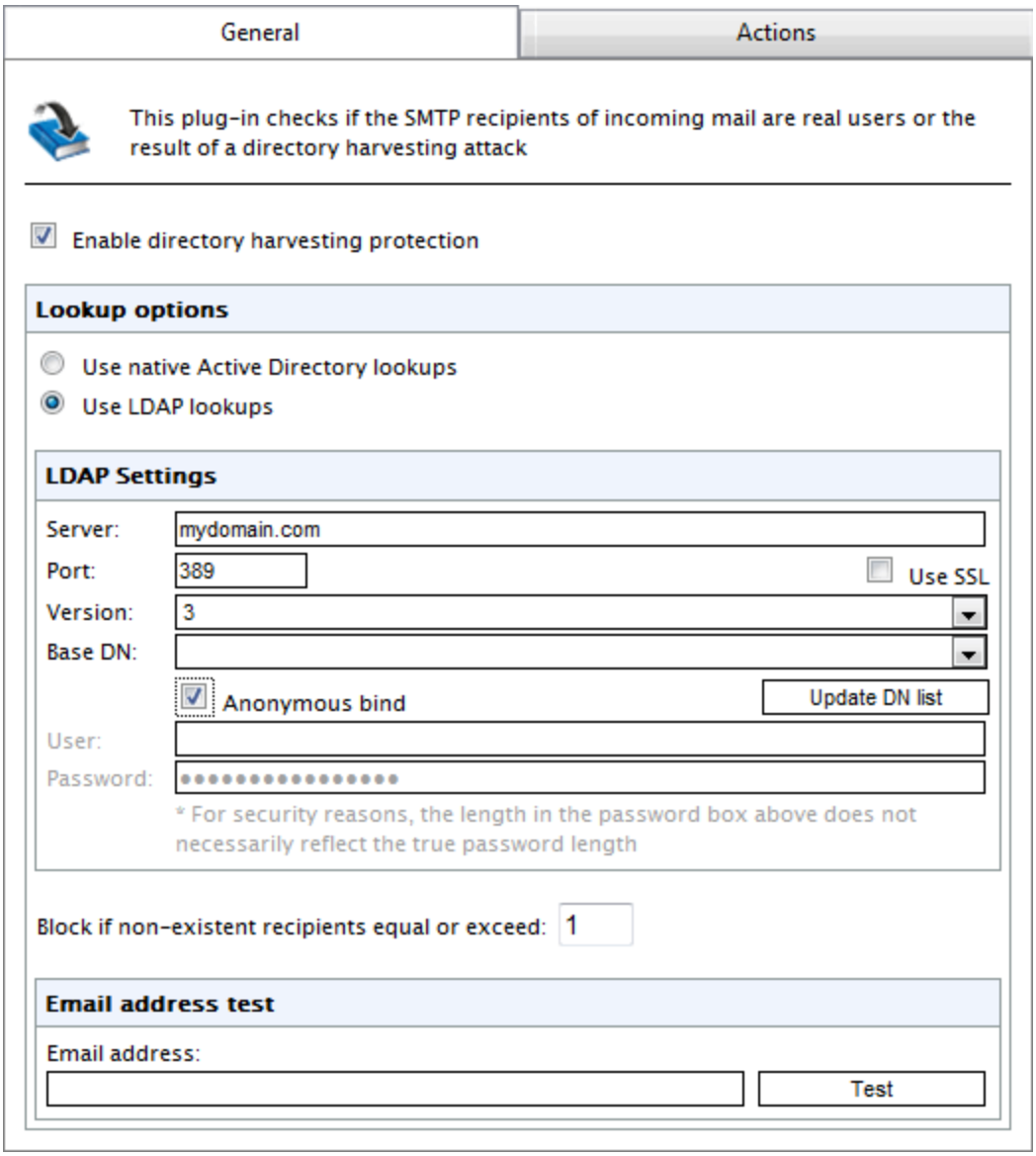
Directory Harvesting is set up in two stages as follows

Stage 1 - Configuring Directory Harvesting properties

Stage 2 - Selecting if Directory Harvesting should be done during the SMTP transmission.

Stage 1 - Configuring Directory Harvesting properties

1. Go to **Anti-Spam > Anti-Spam Filters > Directory Harvesting**.



Screenshot 58: Directory Harvesting page

2. Enable/Disable Directory Harvesting and select the lookup method to use:

Option	Description
Enable directory harvesting protection	Enable/Disable Directory Harvesting.
Use native Active Directory lookups	Select option if GFI MailEssentials is installed in Active Directory. **NOTE** When GFI MailEssentials is behind a firewall, the Directory Harvesting feature might not be able to connect directly to the internal Active Directory because of Firewall settings. Use LDAP lookups to connect to the internal Active Directory of your network and ensure to enable default port 389/636 on your Firewall.

Option	Description
Use LDAP lookups	Select to configure your LDAP settings if GFI MailEssentials is installed in SMTP mode. If your LDAP server requires authentication, unmark the **Anonymous bind** option and enter the authentication details that will be used by this feature. **NOTE** Specify authentication credentials using Domain\User format (for example master-domain\administrator). **NOTE** In an Active Directory, the LDAP server is typically the Domain Controller.

3. In **Block if non-existent recipients equal or exceed**, specify the number of nonexistent recipients that will qualify the email as spam. Emails will be blocked by Directory Harvesting if all the recipients of an email are invalid, or if the number of invalid recipients in an email equals or exceeds the limit specified.

NOTE

Avoid false positives by configuring a reasonable amount in the **Block if non-existent recipients equal or exceed** edit box. This value should account for users who send legitimate emails with mistyped email addresses or to users no longer employed with the company. It is recommended that this value is at least **2**.

4. Provide an email address and click **Test** to verify Directory Harvesting settings. Repeat the test using a non-existent email address and ensure that Active Directory lookup fails.
5. Click **Actions** tab to select the actions to perform on messages identified as spam. For more information, refer to Spam Actions - What to do with spam emails (page 135).

NOTE

If Directory Harvesting is set to run at SMTP level, only the **Log Occurrence** option will be available in the **Actions** tab.

6. Click **Apply**.

Stage 2 - Selecting if Directory Harvesting should be done during the SMTP transmission.

1. Navigate to **Anti-spam > Filter Priority**, and select **SMTP Transmission Filtering** tab.
2. Select an option from the following:

Option	Description
Switch to full email filtering	Filtering is done when the whole email is received.
Switch to SMTP transmission filtering	Filtering is done during SMTP transmission by checking if the email recipients exist before the email body and attachment are received. **NOTE** If this option is chosen, Directory Harvesting will always run before the other spam filters.

3. Click **Apply**.

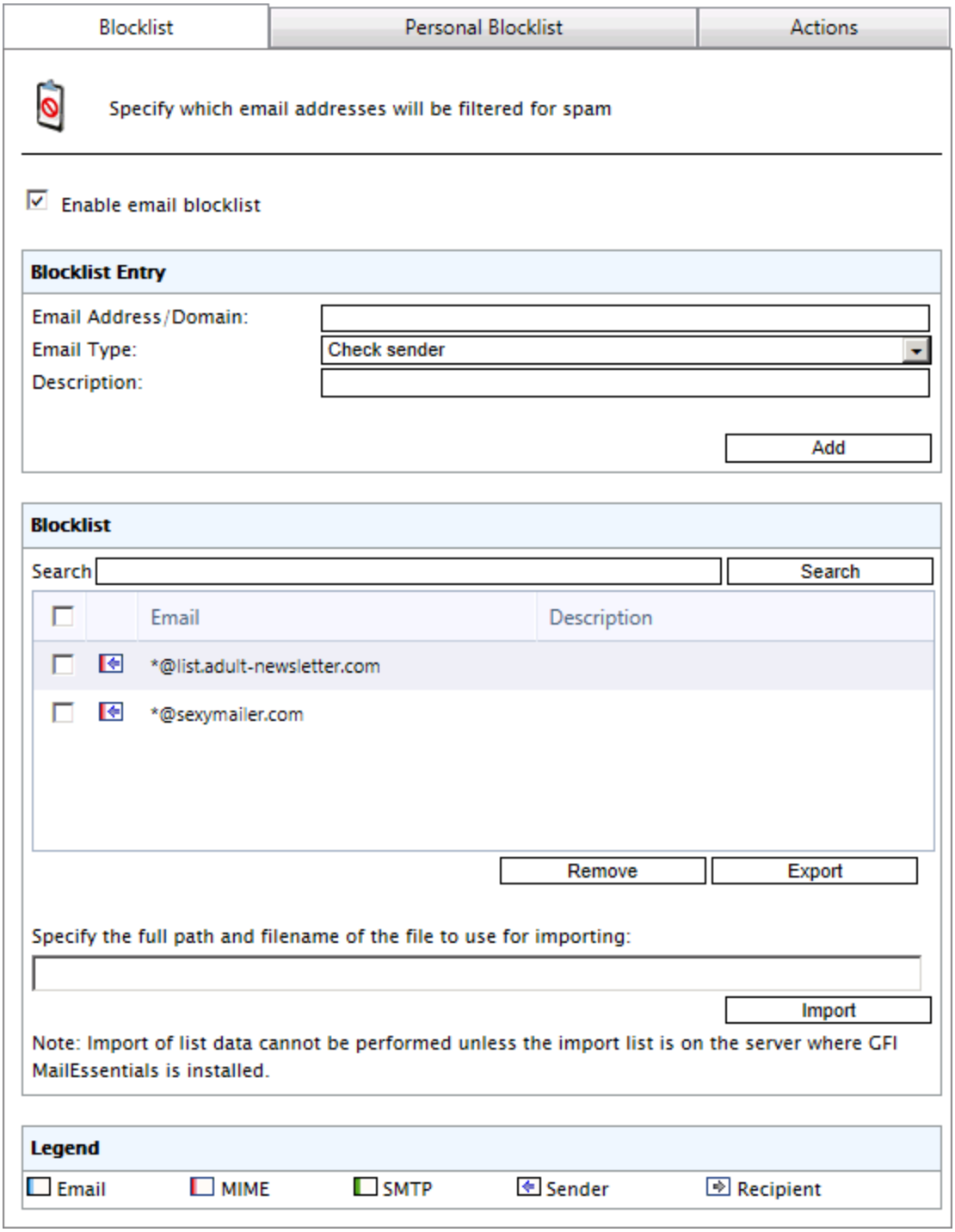
7.1.4 Email blocklist

The Email Blocklist is a custom database of email addresses and domains from which you never want to receive emails.

This filter is enabled by default on installing GFI MailEssentials.

Configuring Email Blocklist

1. Go to **Anti-Spam > Anti-Spam Filters > Email Blocklist**.



Screenshot 59: Email blocklist

2. From the **Blocklist** tab, configure the email addresses and domains to block.

OPTION	DESCRIPTION
Enable Email Blocklist	Select/Unselect to enable/disable email blocklist.
Add	Add email addresses, email domains or an entire domain suffix to the blocklist. 1. Key in an email address, domain (for example, *@spammer.com); or an entire domain suffix (for example *@*.tv) to add to the blocklist. 2. Specify the email type to match for the emails to be blocklisted. **NOTE** For more information about the difference between SMTP and MIME refer to: http://go.gfi.com/?pageid=ME_DifferenceSMTPMIME 3. (Optional) You can also add a description to the entry in the Description field. 4. Click **Add**.
Remove	Select a blocklist entry and click **Remove** to delete.
Import	Import a list of blocklist entries from a file in XML format. **NOTE** A list of entries can be imported from a file in XML format in the same structure that GFI MailEssentials would export the list of entries.
Export	Export the list of blocklist entries to a file in XML format.
Search	Key in an entry to search for. Matching entries are filtered in the list of blocklist entries.

3. Click **Actions** tab to select the actions to perform on messages identified as spam. For more information, refer to Spam Actions - What to do with spam emails (page 135).
4. Click **Apply**.

Personal Blocklist

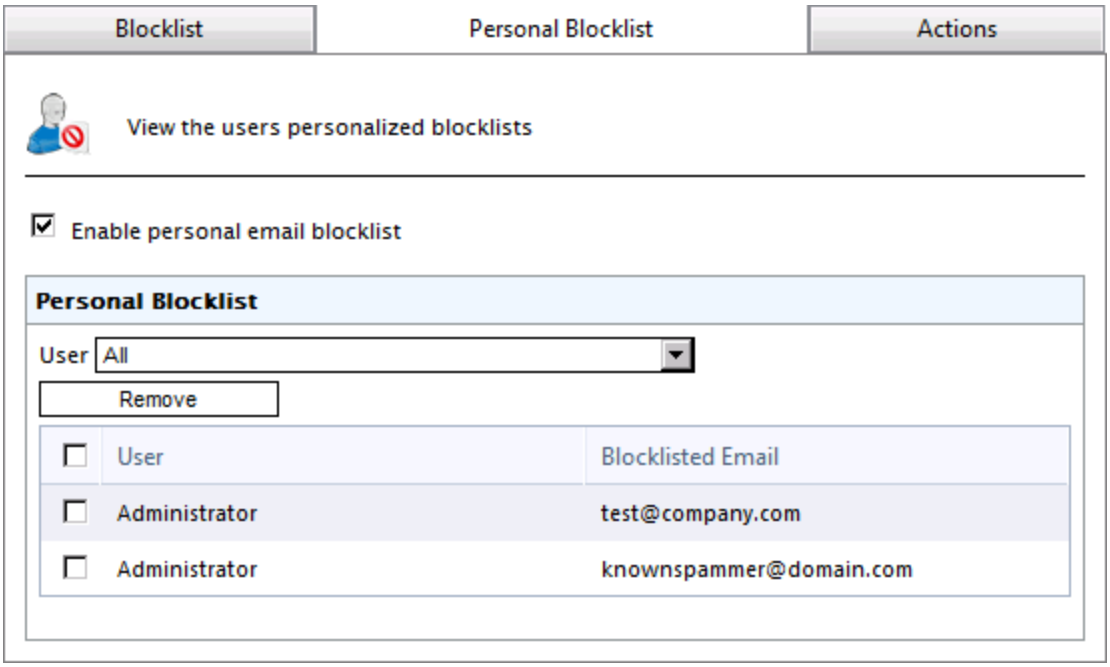
The personal blocklist is an additional blocklist that compliments global blocklist . Disabled by default, the personal blocklist can be enabled for users to enable them to add specific email addresses to a personal blocklist that they can manage. For management purposes, administrators can also remove specific email addresses that the users have added to their personal blocklist.

NOTE

For detailed information on how users can add, delete, export and import personal whitelist and blocklist email addresses, refer to

Enabling/Disabling Personal Blocklist

1. Go to **Anti-Spam > Email Blocklist**.



Screenshot 60: Personal blocklist

2. Select **Personal Blocklist** tab and select or unselect **Enable personal email blocklist** to enable or disable personal blocklist feature.
3. Click **Apply**.

Removing emails from users' personal blocklist

1. Go to **Anti-Spam > Email Blocklist** and select **Personal Blocklist** tab.
2. From the **User** drop down list, select the user for whom to delete an email address.
3. Select an email address from the list of email addresses. Click **Remove**.
4. Click **Apply**.

7.1.5 IP DNS Blocklist

IP DNS Blocklist checks the IP address of the sending mail server against a public list of mail servers known to send spam. GFI MailEssentials supports a number of IP DNS Blocklists. There are a number of third party IP DNS Blocklists available, ranging from reliable lists that have clearly outlined procedures for getting on or off the IP DNS Blocklist to less reliable lists.

GFI MailEssentials maintains a cache with the results of queries to the IP DNS Blocklist to avoid querying the IP DNS Blocklists multiple times for the same IP addresses. Items remain in the cache for 4 days and are cleared on GFI MailEssentials AS Scan Engine service restart.

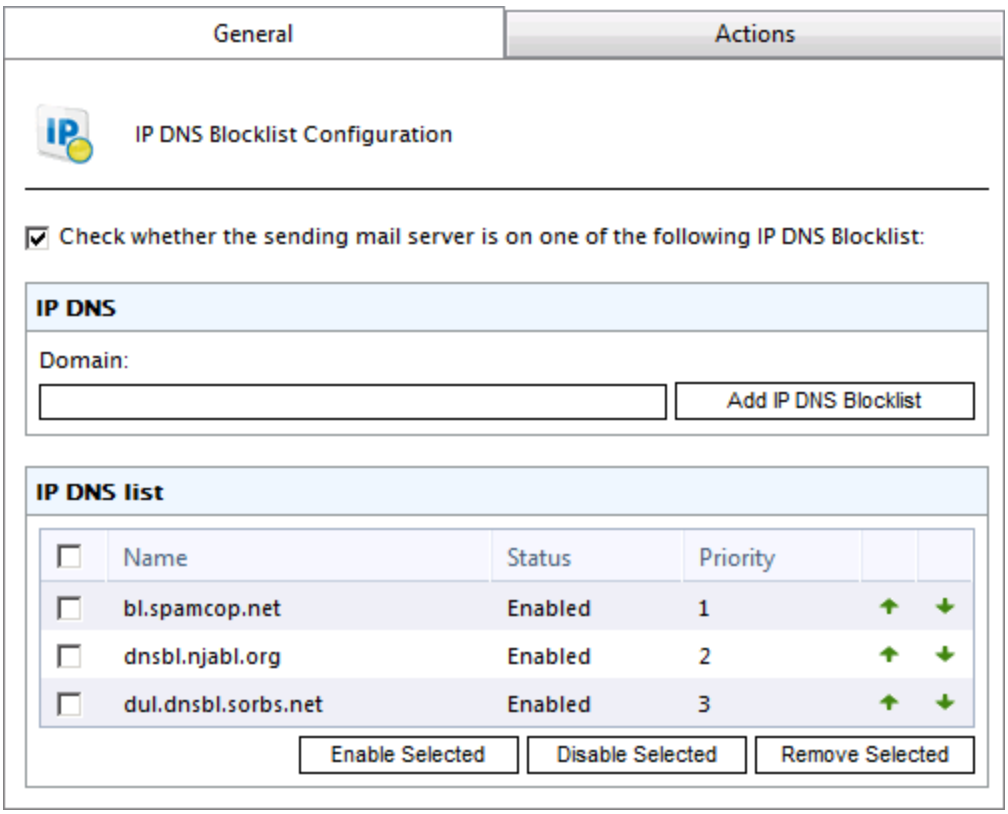
This filter is enabled by default on installing GFI MailEssentials.

Important notes

1. The DNS server must be properly configured for this feature to work. If this is not the case, time outs will occur and email traffic will be slowed down. For more information refer to: http://go.gfi.com/?pageid=ME_ProcessingSlow
2. Querying an IP DNS Blocklist can be slow (depending on your connection), so email can be slowed down a little bit.
3. Ensure that all perimeter SMTP servers are configured in the Perimeter SMTP servers dialog so that GFI MailEssentials can check the IP address that is connecting to the perimeter servers. For more information, refer to Perimeter SMTP Server Settings (page 148).

Configuring IP DNS Blocklist

1. Go to **Anti-Spam > Anti-Spam Filters > IP DNS Blocklist**.



Screenshot 61: IP DNS Blocklist

2. Configure the following options:

Option	Description
Check whether the sending mail server is on one of the following IP DNS Blocklists:	Select to enable the IP DNS Blocklist filter.
Add IP DNS Blocklist	If required, add more IP DNS Blocklists to the ones already listed. Key in the IP DNS Blocklist domain and click **Add IP DNS Blocklist**.
Enable Selected	Select an IP DNS Blocklist and click **Enable Selected** to enable it.
Disable Selected	Select an IP DNS Blocklist and click **Disable Selected** to disable it.
Remove Selected	Select an IP DNS Blocklist and click **Remove Selected** to remove it.

3. Click **Actions** tab to select the actions to perform on messages identified as spam. For more information, refer to Spam Actions - What to do with spam emails (page 135).
4. Click **Apply**.

> **NOTE**
>
> To enable IP DNS Blocklist at SMTP Transmission Filtering level, select **Anti-Spam > Filter Priority > SMTP Transmission Filtering** tab and click **Switch** next to IP DNS Blockist to enable/disable filtering at SMTP level or on receipt of full email.

7.1.6 URI DNS Blocklist

Stops emails that contain links to domains listed on public Spam URI Blocklists.

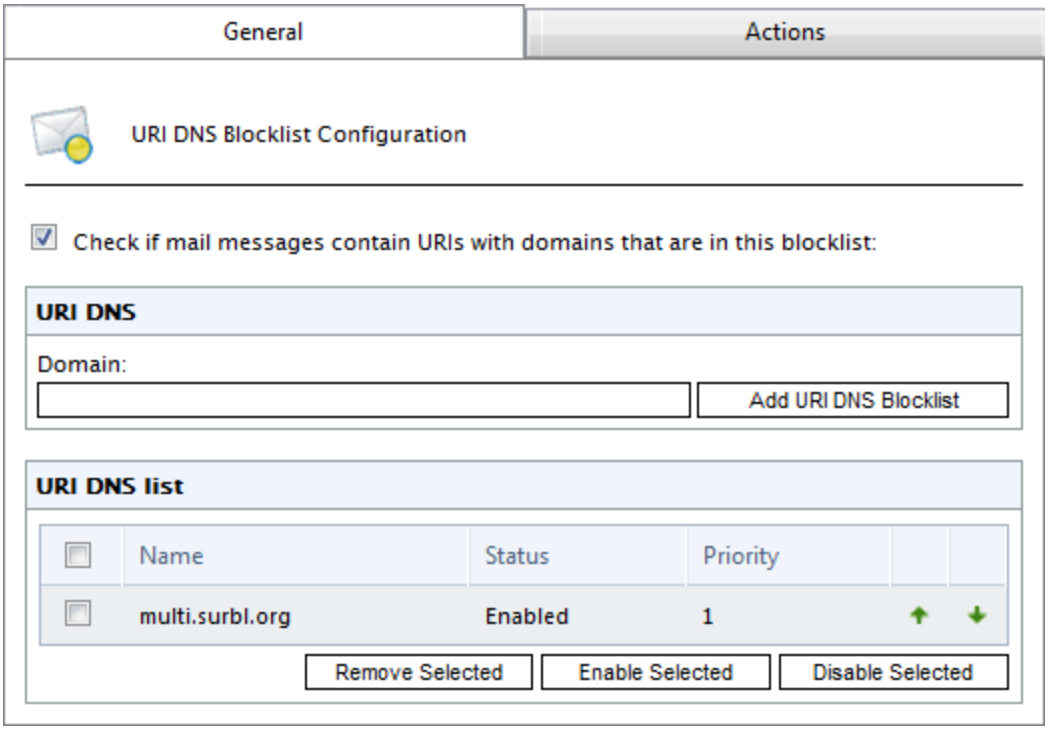
A Universal Resource Identifier (URI) is a standard means of addressing resources on the Web.

Realtime Blocklists (RBL) detect spam based on hyperlinks in the email known to be used by spammers.

This filter is enabled by default on installing GFI MailEssentials.

Configuring URI DNS Blocklist

1. Go to **Anti-Spam > Anti-Spam Filters > URI DNS Blocklist**.



Screenshot 62: URI DNS Blocklist

2. From the **URI DNS Blocklist** tab:

Option	Description
Check if mail message contains URIs with domains that are in these blocklists:	Select this option to enable the URI DNS Blocklist filter.

Option	Description
Add URI DNS Blocklist	If required, add more URI DNS Blocklists to the ones already listed. Key in the full name of the URI DNS Blocklist domain and click **Add URI DNS Blocklist**.
Order of preference	The order of preference for enabled URI DNS Blocklists can be changed by selecting a blocklist and clicking on the Up or Down buttons.
Enable Selected	Select a URI DNS Blocklist and click **Enable Selected** to enable it. **NOTE** It is recommended to disable all other URI DNS Blocklists when enabling **multi.surbl.org** as this might increase email processing time.
Disable Selected	Select a URI DNS Blocklist and click **Disable Selected** to disable it.
Remove Selected	Select a URI DNS Blocklist and click **Remove Selected** to remove it.

3. Click **Actions** tab to select the actions to perform on messages identified as spam. For more information, refer to Spam Actions - What to do with spam emails (page 135).
4. Click **Apply**.

7.1.7 Sender Policy Framework

This filter uses SPF records to stop email sent from forged IP addresses by identifying if the sender IP address is authorized. The Sender Policy Framework filter is based on a community-based effort, which requires that the senders publish the IP addresses of their mail servers in an SPF record.

Example: If an email is sent from xyz@CompanyABC.com then companyABC.com must publish an SPF record in order for SPF to be able to determine if the email was really sent from the companyABC.com network or whether it was forged. If an SPF record is not published by CompanyABC.com, the SPF result will be 'unknown'.

For more information on SPF and how it works, visit the Sender Policy Framework website at:

http://www.openspf.org.

The SPF filter is NOT enabled by default and it is recommended to enable this option and to have this filter running prior to the Email Whitelist so to block forged senders before these are whitelisted.

GFI MailEssentials does not make it a requirement to publish any SPF records. To publish SPF records use the SPF wizard at:

http://www.openspf.org/wizard.html.

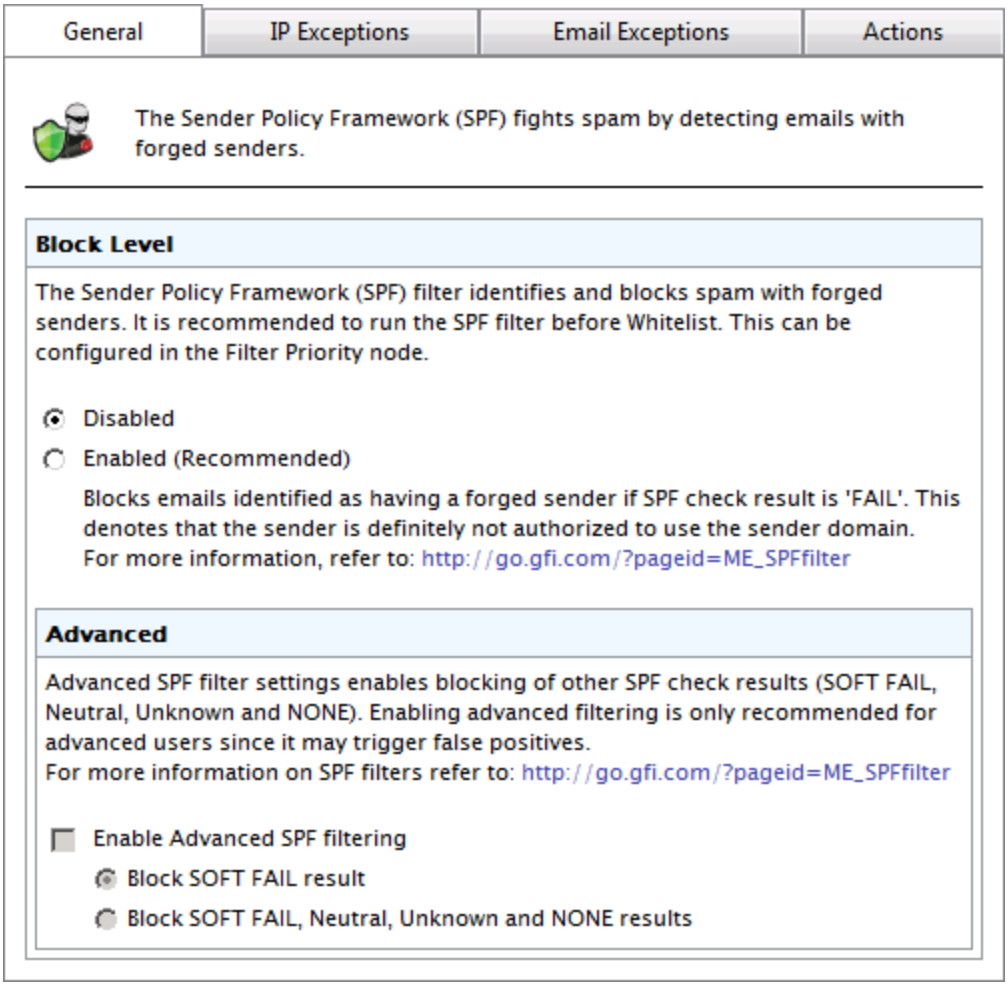
Prerequisites

Before enabling the Sender Policy Framework filter on a non-gateway server installation:

1. Click **Anti-spam > Anti-Spam Settings** and select Perimeter SMTP Servers tab.
2. Click **Detect** in the Perimeter SMTP setup option to perform a DNS MX lookup and automatically define the IP address of your perimeter SMTP server.

Enabling the Sender Policy Framework

1. Select **Anti-Spam > Anti-Spam Filters > Sender Policy Framework**.


General
IP Exceptions
Email Exceptions
Actions
The Sender Policy Framework (SPF) fights spam by detecting emails with forged senders.
Block Level
The Sender Policy Framework (SPF) filter identifies and blocks spam with forged senders. It is recommended to run the SPF filter before Whitelist. This can be configured in the Filter Priority node.
Disabled
Enabled (Recommended)
Blocks emails identified as having a forged sender if SPF check result is 'FAIL'. This denotes that the sender is definitely not authorized to use the sender domain.
For more information, refer to: http://go.gfi.com/?pageid=ME_SPFfilter
Advanced
Advanced SPF filter settings enables blocking of other SPF check results (SOFT FAIL, Neutral, Unknown and NONE). Enabling advanced filtering is only recommended for advanced users since it may trigger false positives.
For more information on SPF filters refer to: http://go.gfi.com/?pageid=ME_SPFfilter
Enable Advanced SPF filtering
Block SOFT FAIL result
Block SOFT FAIL, Neutral, Unknown and NONE results

Screenshot 63: Enable and configure the Sender Policy Framework

2. Click **Enabled** to enable the Sender Policy Framework filter. If the email sender IP address is definitely not authorized to send emails from the sender domain, emails are blocked.

3. Optionally, select **Enable Advanced SPF filtering** and select one of the advanced option from:

OPTION	DESCRIPTION
Block SOFT FAIL result	Blocks all emails which: » Sender IP address is definitely not allowed to send emails from the sender domain » Sender IP address is probably not allowed to send emails from the sender domain. For more information on Advanced SPF filtering, refer to: http://go.gfi.com/?pageid=ME_SPFfilter
Block SOFT FAIL, Neutral, Unknown and NONE results	Blocks all emails which: » Sender IP address is definitely not allowed to send emails from the sender domain » Sender IP address is probably not allowed to send emails from the sender domain. » Sender IP address is explicitly inconclusive, unknown or for which there is no published data. For more information on Advanced SPF filtering, refer to: http://go.gfi.com/?pageid=ME_SPFfilter

4. Select **IP Exceptions** or **Email Exceptions** tab to configure IP addresses and/or recipients to exclude from SPF checks:

» **IP exception list:** Entries in this list automatically pass SPF checks. Select **IP Exception List** checkbox,add a new IP address and description and click **Add**. To remove entries, select entries from the list and click **Remove Selected**. To disable the IP exception list unselect **IP Exception List** checkbox.

> **NOTE**
>
> When adding IP addresses to the IP exception list, you can also add a range of IP addresses using the CIDR notation.

» **Email exception list:** This option ensures that certain email senders or recipients are excluded from SPF checking, even if the messages are rejected.Select **Email Exception List** checkbox,add a new email address and description and click **Add**. To remove entries, select entries from the list and click **Remove Selected**. To disable the Email exception list unselect **Email Exception List** checkbox. An email address can be entered in any of the following three ways:

- localpart - 'abuse' (matches 'abuse@abc.com', 'abuse@xyz.com', etc...)
- domain - '@abc.com' (matches 'john@abc.com', 'jill@abc.com', etc...)
- complete - 'joe@abc.com' (only matches 'joe@abc.com')

5. Click **Actions** tab to select the actions to perform on messages identified as spam. For more information, refer to Spam Actions - What to do with spam emails (page 135).
6. Click **Apply** to save settings.

7.1.8 Anti-Spoofing

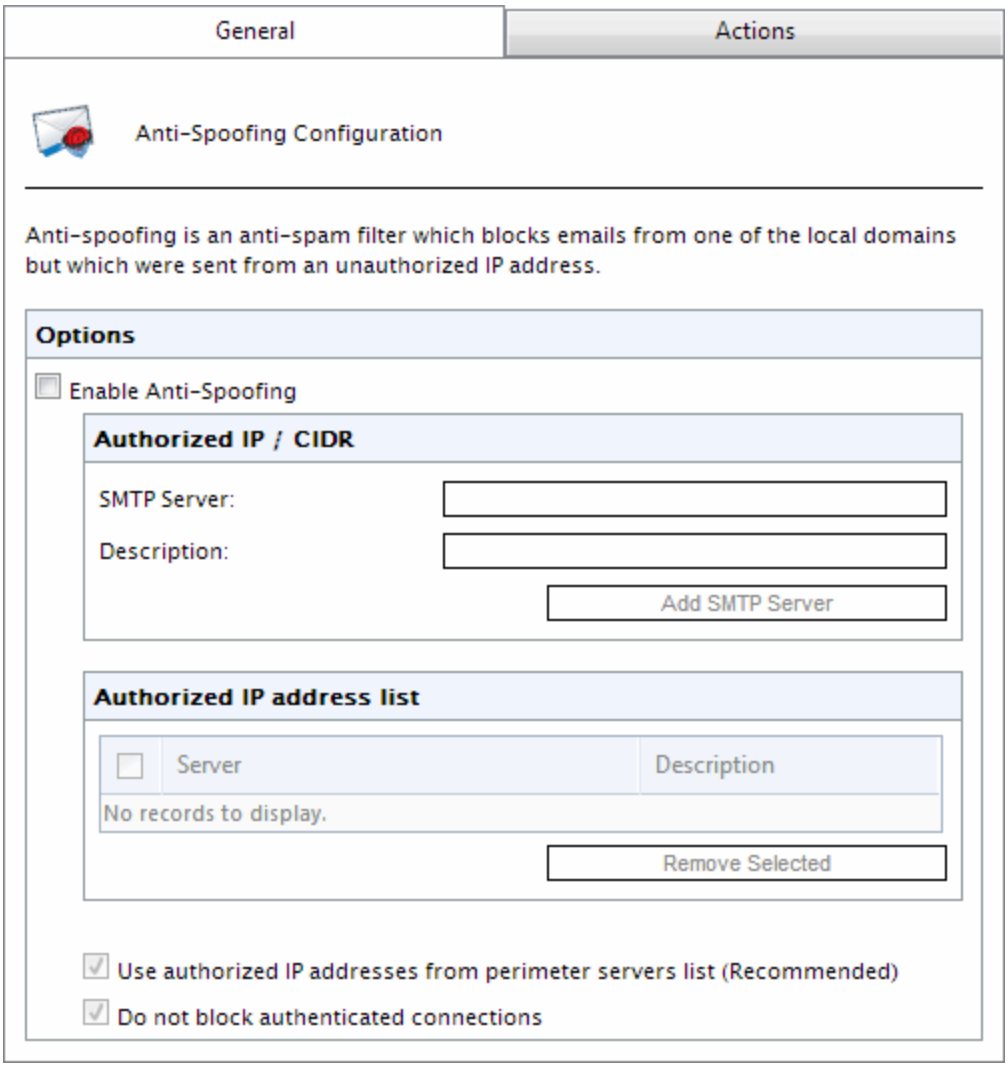
Checks emails received with a sender email address claiming to originate from your own domain against a list of IP addresses by GFI MailEssentials. If the sender IP address is not on the list of own-domain server IP addresses, email is blocked.

This filter is NOT enabled by default.

> **WARNING**
>
> If enabling this feature do not whitelist internal users since this defeats Anti-Spoofing check.

Enabling and configuring Anti-Spoofing

1. Go to **Anti-Spam > Anti-Spam Filters > Anti-Spoofing**.



Screenshot 64: GFI MailEssentials Anti-Spoofing filter

2. Select **Enable Anti-Spoofing** to enable Anti-Spoofing filter.
3. In the **SMTP Server:** field, provide the SMTP server where GFI MailEssentials checks for email recipient addresses. Also provide a description for the server in the **Description:** field.

NOTE

The SMTP Server field supports the following types of entry:

- A single IP Address
- A CIDR range (for example, 192.0.2.1/24)

4. Click **Add SMTP Server** to save SMTP server details.

NOTE

To remove previously added SMTP servers, select an SMTP server from the Authorized IP Address list and click **Remove Selected**.

By default, **Use authorized IP addresses from perimeter server** and **Do not block authenticated connections** are enabled. It is not recommended that these options are disabled.

> **NOTE**
>
> **Do not block authenticated connections** check boxdoes not apply for Microsoft IIS and Microsoft Exchange 2003. It only works with Exchange 2007 or later.

7.1.9 Greylist

The Greylist filter temporarily blocks incoming emails received from unknown senders. Legitimate mail systems typically try to send the email after a few minutes; spammers simply ignore such error messages. If an email is received again after a predefined period, Greylist will:

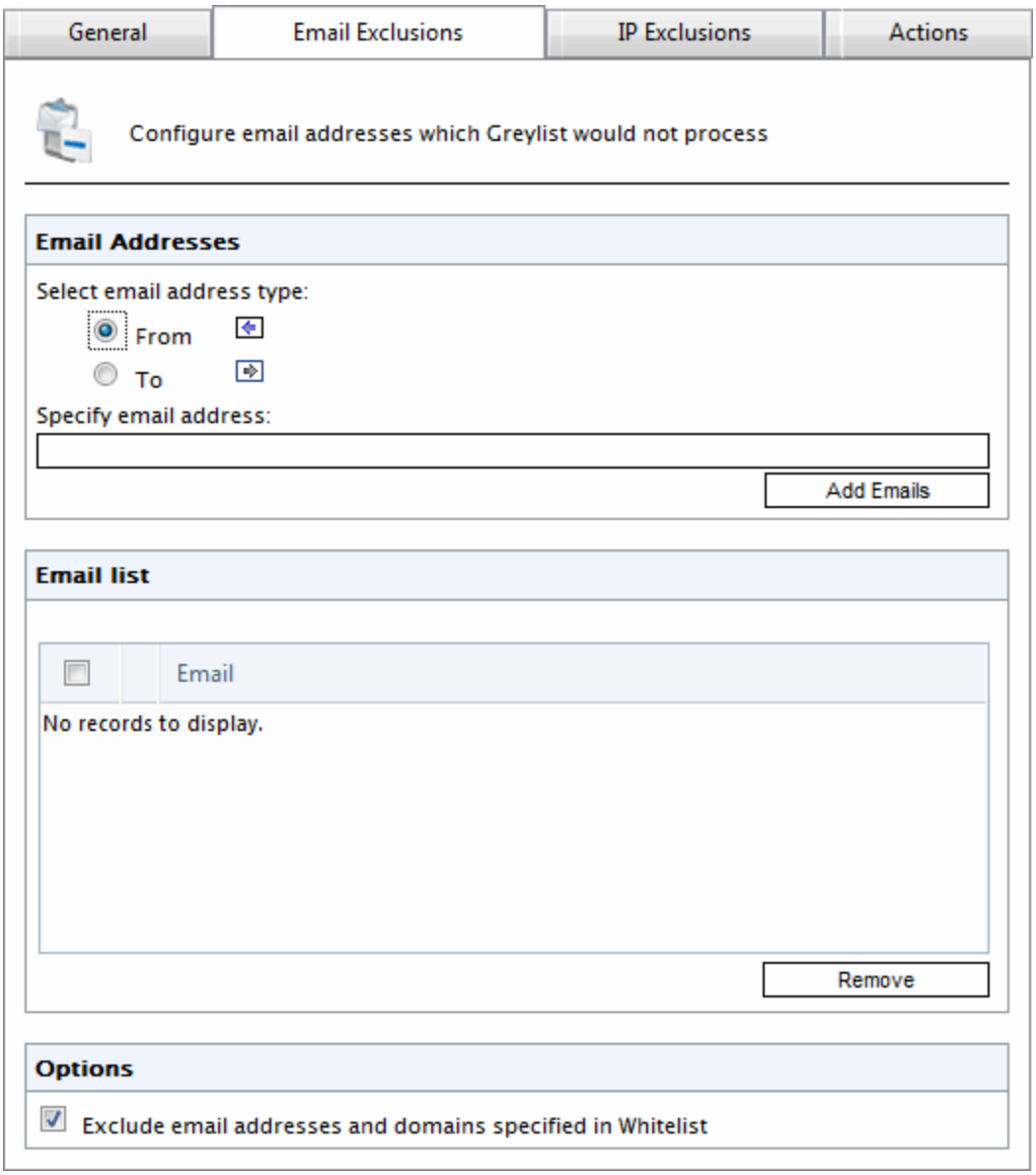
- Store the details of the sender in a database so that when the sender sends another email, the email will not be greylisted
- Receive the email and proceed with anti-spam scanning

Greylist is **NOT** enabled by default.

> **Important Notes**
>
> 1. To enable Greylist, GFI MailEssentials must be installed on the perimeter SMTP server. For more information refer to http://go.gfi.com/?pageid=ME_GreylistSMTP
> 2. Greylist contains exclusion lists so that specific email addresses, domains and IP addresses are not greylisted. Exclusions must be configured when:
>
> - Emails originating from particular email addresses, domains or IP addresses cannot be delayed
> - Emails addressed to a particular local user cannot be delayed

Configuring Greylist

1. Go to **Anti-Spam > Anti-Spam Filters > Greylist**.
2. From the **General** tab select/unselect **Enable Greylist** to enable/disable Greylist.



Screenshot 65: Email Exclusions

3. Select **Email exclusions** tab to specify any email addresses or domains that you do not want to greylist. In the **Edit Addresses** area specify:

» full email address; or

» emails from an entire domain (for example: *@trusteddomain.com); or

» an entire domain suffix (for example: *@*.mil or *@*.edu)

Also specify if the exclusion applies to senders (select **From (>)**) or to the local recipients (select **To (>)**).

» **Example 1:** Do not greylist emails if the recipient is administrator@mydomain.com, so that any emails sent to administrator@mydomain.com are never delayed.

» **Example 2:** Do not greylist emails if the sender's domain is trusteddomain.com (`*@trusteddomain.com`), so that emails received from domain trusteddomain.com are never delayed.

Click **Add emails** to add the exclusion.

NOTE

To exclude whitelisted and auto-whitelisted email addresses and domains from being greylisted and delayed, select **Exclude email addresses and domains specified in Whitelist**.

4. Select the **IP exclusions** tab to specify any IP addresses to exclude from being greylisted. Click **Add IPs** and specify an IP to exclude.
5. To exclude whitelisted IP addresses from being greylisted and delayed, select **Exclude IP addresses specified in Whitelist**.
6. To log Greylist occurrences to a log file, click **Actions** tab and select **Log occurrence to this file**.

NOTE

Log files may become very large. GFI MailEssentials supports log rotation, where new log files are created periodically or when the log file reaches a specific size. To enable log file rotation navigate to **Anti-Spam > Anti-Spam Settings**. Select **Anti-spam logging** tab, check **Enable log file rotation** and specify the rotation condition.

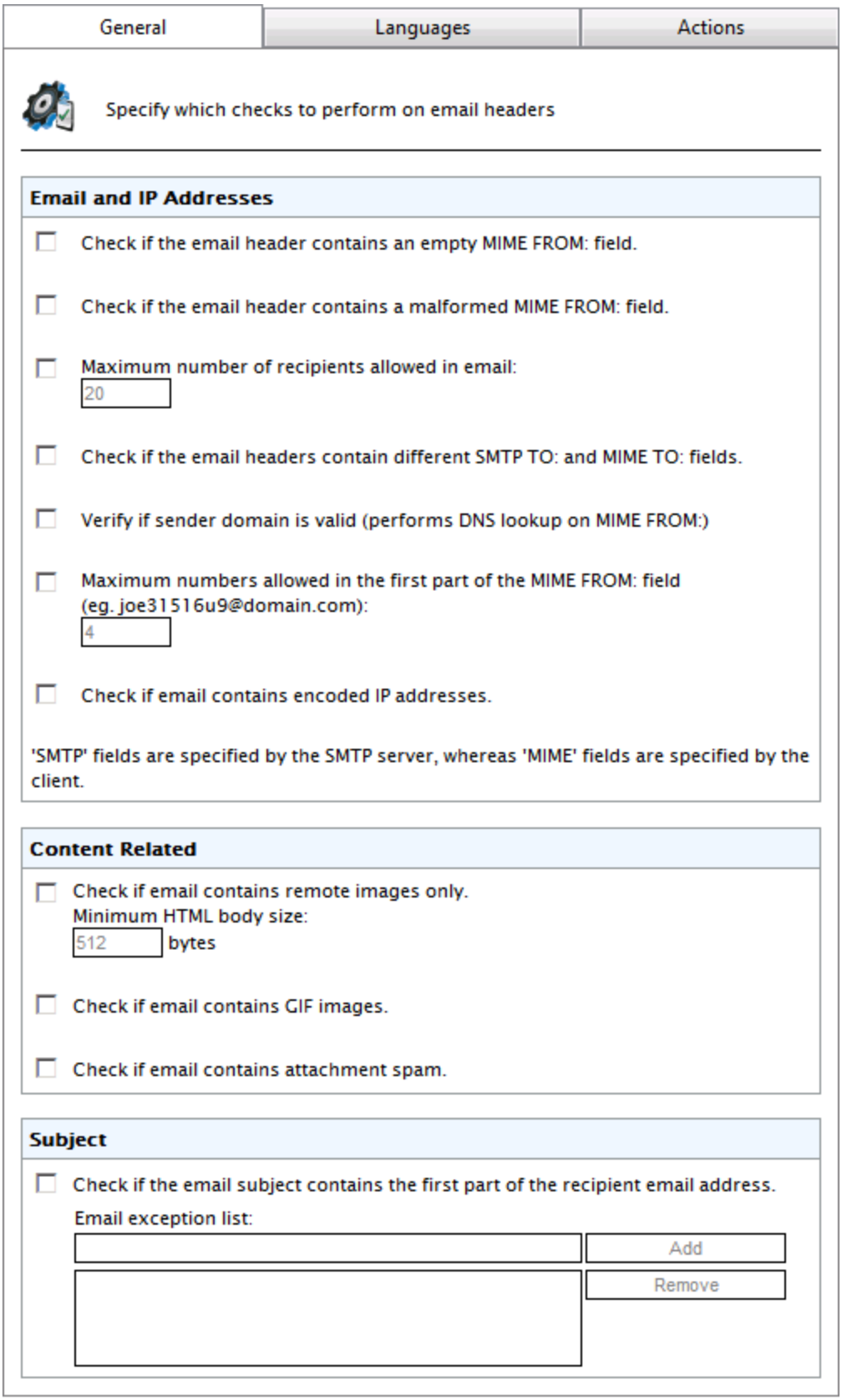
7. Click **Apply**.

7.1.10 Header Checking

The Header Checking filter analyses the email header to identify spam emails.

Configuring Header Checking

1. Go to **Anti-Spam > Anti-Spam Filters > Header Checking**.

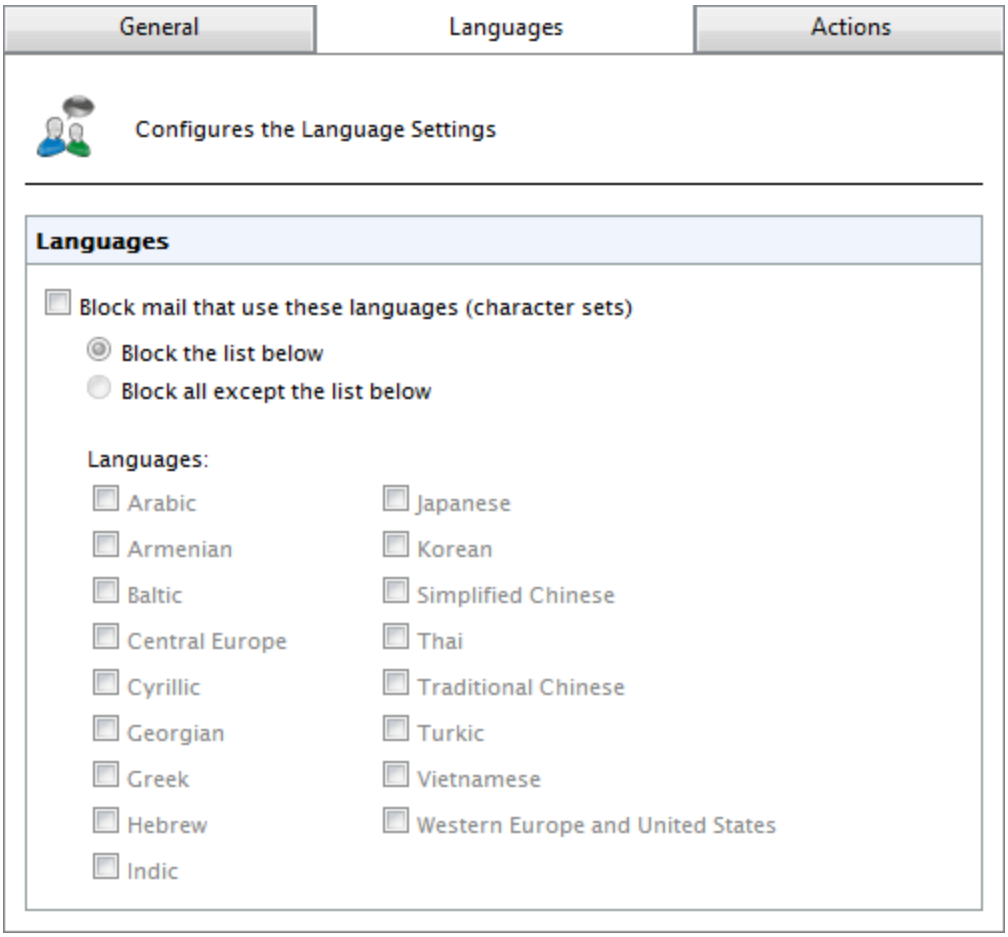

General
Languages
Actions
Specify which checks to perform on email headers
Email and IP Addresses
Check if the email header contains an empty MIME FROM: field.
Check if the email header contains a malformed MIME FROM: field.
Maximum number of recipients allowed in email:
20
Check if the email headers contain different SMTP TO: and MIME TO: fields.
Verify if sender domain is valid (performs DNS lookup on MIME FROM:)
Maximum numbers allowed in the first part of the MIME FROM: field (eg. joe31516u9@domain.com):
4
Check if email contains encoded IP addresses.
'SMTP' fields are specified by the SMTP server, whereas 'MIME' fields are specified by the client.
Content Related
Check if email contains remote images only.
Minimum HTML body size:
512
bytes
Check if email contains GIF images.
Check if email contains attachment spam.
Subject
Check if the email subject contains the first part of the recipient email address.
Email exception list:
Add
Remove

Screenshot 66: Header checking options

2. Enable, disable or configure the following parameters:

Option	Description
Check if the email header contains an empty MIME FROM: field.	Checks if the sender has identified himself in the From: field. If this field is empty, the message is marked as spam.
Check if the email header contains a malformed MIME FROM: field.	Checks if the MIME from field is a correct notation as defined in the RFCs.
Maximum number of recipients allowed in email	Identifies emails with large amounts of recipients and flags them as SPAM.
Check if the email headers contain different SMTP TO: and MIME TO: fields.	Checks whether the SMTP to: and MIME to: fields are the same. The spammers email server always has to include an SMTP to: address. However, the MIME to: email address is often not included or is different. **NOTE:** This feature identifies a lot of spam, however some list servers do not include the MIME to: either. It is therefore recommended to whitelist newsletter sender address to use this feature.
Verify if sender domain is valid (performs DNS lookup on MIME FROM:)	Performs a DNS lookup on the domain in the MIME from field and verifies the domain validity. **NOTE:** Ensure that the DNS server is properly configured to avoid timeouts and slow email flow.
Maximum numbers allowed in the first part of the MIME FROM: field:	Identifies the presence of numbers in the MIME from field. Spammers often use tools that automatically create unique reply-to: addresses by using numbers in the address.
Check if email contains encoded IP addresses.	Checks the message header and body for URLs which have a hex/octal encoded IP (http://0072389472/hello.com) or which have a username/password combination (for example www.citibank.com@scammer.com). The following examples are flagged as spam: » http://12312 » www.microsoft.com:hello%01@123123
Check if email contains remote images only. Minimum HTML body size	Flag emails that only have remote images and a minimal amount of text as spam. Assists in identifying 'image only email' spam.
Check if email contains GIF images.	Checks if the email contains one or more embedded GIF images. Embedded GIF images are often used to circumvent spam filters. **IMPORTANT:** **Since some legitimate emails contain embedded GIF images, this option is prone to false positives.**
Check if email contains attachment spam.	Checks email attachments for properties that are common to attachments sent in spam email. This helps in keeping up with the latest techniques used by spammers in using attachments to send spam.
Check if the email subject contains the first part of the recipient email address.	Identifies the personalized spam email, where spammers frequently include the first part of the recipient email address in the subject.

3. From the **Language** tab, select **Block mail that use these languages (character sets)** to enable language detection.



Screenshot 67: Language Detection

4. Select **Block the list below** to select the languages to block or **Block all except the list below** to block all languages except the ones selected.
5. Select the languages to block/allow from the **Languages** area.
6. Click **Actions** tab to select the actions to perform on messages identified as spam. For more information, refer to Spam Actions - What to do with spam emails (page 135).
7. Click **Apply**.

7.1.11 Spam Keyword Checking

This filter enables the identification of Spam based on keywords in the email being received.

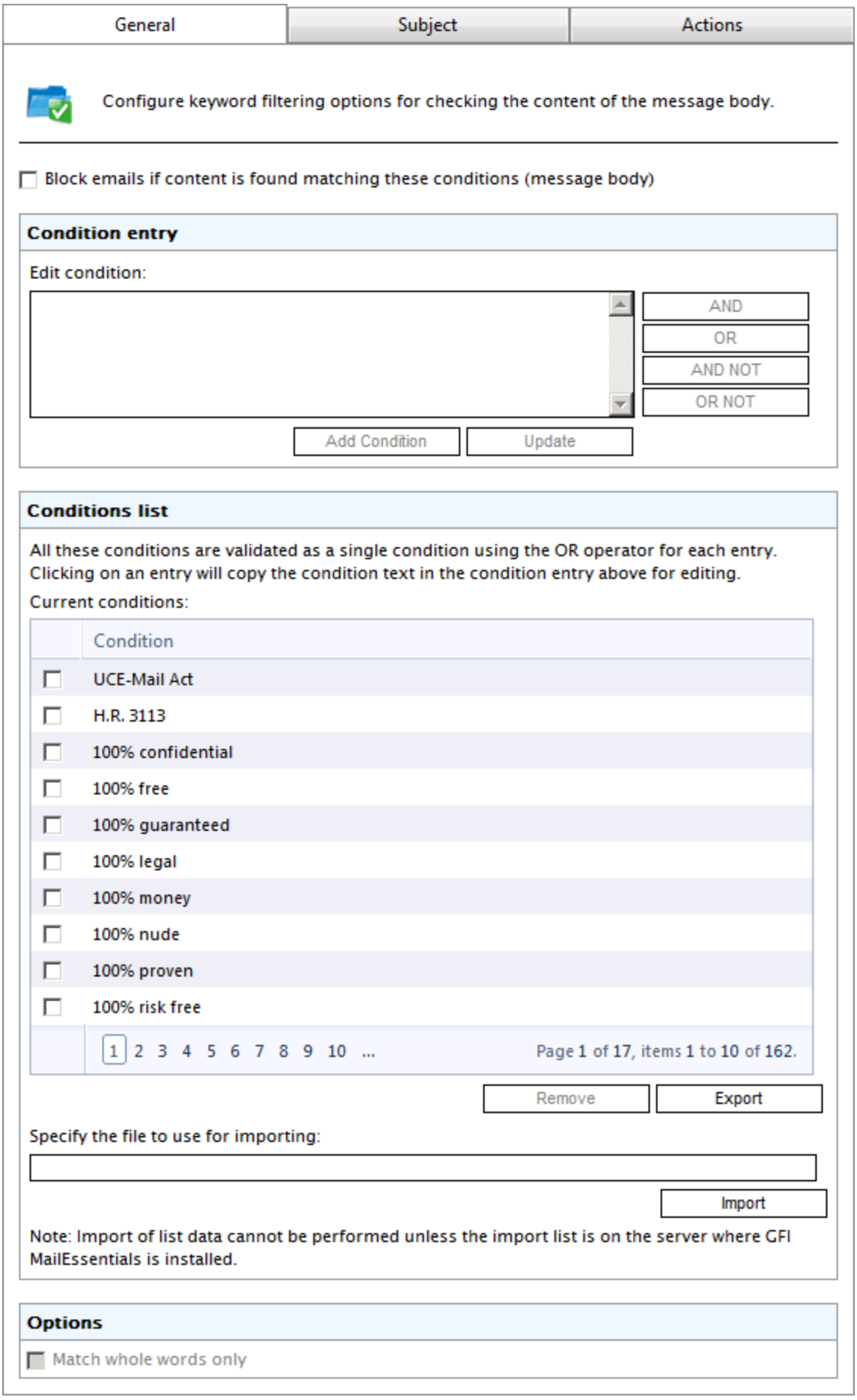
This filter is **NOT** enabled by default on installing GFI MailEssentials.

> **NOTE**
>
> This filter only checks the content of the email for text that identifies the email as Spam. For comprehensive content filtering of email (for example to block Racial content or Profanities), use the Keyword filtering option within the Content Filtering node.

Add Spam Keyword Check

1. Go to **Anti-Spam > Anti-Spam Filters > Spam Keyword Checking**.

2. From the **General** tab, select **Block emails if content is found matching these conditions (message body)** to enable Spam Keyword checking on email body.


General
Subject
Actions
Configure keyword filtering options for checking the content of the message body.
Block emails if content is found matching these conditions (message body)
Condition entry
Edit condition:
AND
OR
AND NOT
OR NOT
Add Condition
Update
Conditions list
All these conditions are validated as a single condition using the OR operator for each entry.
Clicking on an entry will copy the condition text in the condition entry above for editing.
Current conditions:
Condition
UCE-Mail Act
H.R. 3113
100% confidential
100% free
100% guaranteed
100% legal
100% money
100% nude
100% proven
100% risk free
1 2 3 4 5 6 7 8 9 10 ...
Page 1 of 17, items 1 to 10 of 162.
Remove
Export
Specify the file to use for importing:
Import
Note: Import of list data cannot be performed unless the import list is on the server where GFI MailEssentials is installed.
Options
Match whole words only

Screenshot 68: Spam Keyword checking properties

3. In the **Condition Entry** area, key in a keyword or a combination of keywords for this filter to block. Use the 'AND', 'OR', 'AND NOT' and 'OR NOT' operators to configure specific conditions.

   For example:

   Key in the phrase‘Basketball sports’, GFI MailEssentials to block an email with the phrase 'Basketball sports'. Only this phrase would activate the rule, not the word basketball OR sports separated by some other words.

   Key in Basketball AND Baseball and GFI MailEssentials will block emails that have both words in the email. Emails with only Basketball or only baseball will not be blocked.

4. Select **Match whole words only** to search specifically for whole words and avoid blocking words that are part of other words. For example, enabling this option would not block the word 'MSExchange', notwithstanding the fact that the word 'sex' is part of 'MSExchange'.
5. Select **Subject** tab, select **Block emails if content is found matching these conditions (message subject)** to enable Spam Keyword checking on email subject.
6. In the **Condition Entry** area, key in a keyword or a combination of keywords for this filter to block. Use the 'AND', 'OR', 'AND NOT' and 'OR NOT' operators to configure specific conditions.
7. Select **Apply the keywords list to also scan senders' display names** to check the display name of the sender email, which can contain spam keywords. For example, Viagra spam, which often has forged senders and the word Viagra in the s
8. Click **Actions** tab to select the actions to perform on messages identified as spam. For more information, refer to Spam Actions - What to do with spam emails (page 135).
9. Click **Apply**.

Removing conditions

To remove a Spam Keyword Checking condition:

1. From the **Conditions list** area within the **General** or **Subject** tab, select one or more conditions to remove.

> **NOTE**
>
> To find the condition to remove, use the controls under the list of conditions to move between the pages listing the conditions.

2. Click **Remove** and **Apply**.

Importing and Exporting conditions

To export more conditions:

1. From the **Conditions list** area within the **General** or **Subject** tab, select one or more conditions to export.

> **NOTE**
>
> To find the conditions to export, use the controls under the list of conditions to move between the pages listing the conditions.

2. In the **File Download** screen, click **Save** and select a folder where to save the export file.

To import conditions:

1. From the **Conditions** list area within the **General** or **Subject** tab, key in the folder and filename of the file to import.
2. Click **Import**.

7.1.12 Bayesian Analysis

An anti-spam filter that can be trained to accurately determine if an email is spam based on past experience.

This manual also contains information how the Bayesian filter works and how it can be trained. For more information, refer to Appendix 1 - Bayesian Filtering (page 265).

The Bayesian Analysis filter is **NOT** enabled by default.

> **IMPORTANT**
>
> Enable learning from outbound emails and allow at least a week for before enabling filter. This is required because the Bayesian filter acquires its highest detection rate when it adapts to your email patterns.

Configuring the Bayesian filter

Configuring the Bayesian filter requires 2 stages:

Stage 1: Training the Bayesian filter

Stage 2: Enabling the Bayesian filter

Stage 1: Training the Bayesian filter

The Bayesian filter can be trained in two ways:

Method 1: Automatically, through outbound emails.

GFI MailEssentials processes legitimate email (ham) by scanning outbound emails. The Bayesian filter can be enabled after it has collected at least 500 outbound emails (If you send out mainly English email) or 1000 outbound mails (If you send out non-English email).

To do this:

1. Go to **Anti-Spam > Anti-Spam Filters > Bayesian Analysis**.

2. Select **Automatically learn from outbound e-mails**.

3. Click **Apply**.

Method 2: Manually, through existing email.

Copying between 500-1000 mails from your sent items to the **This is legitimate email** sub folder in the

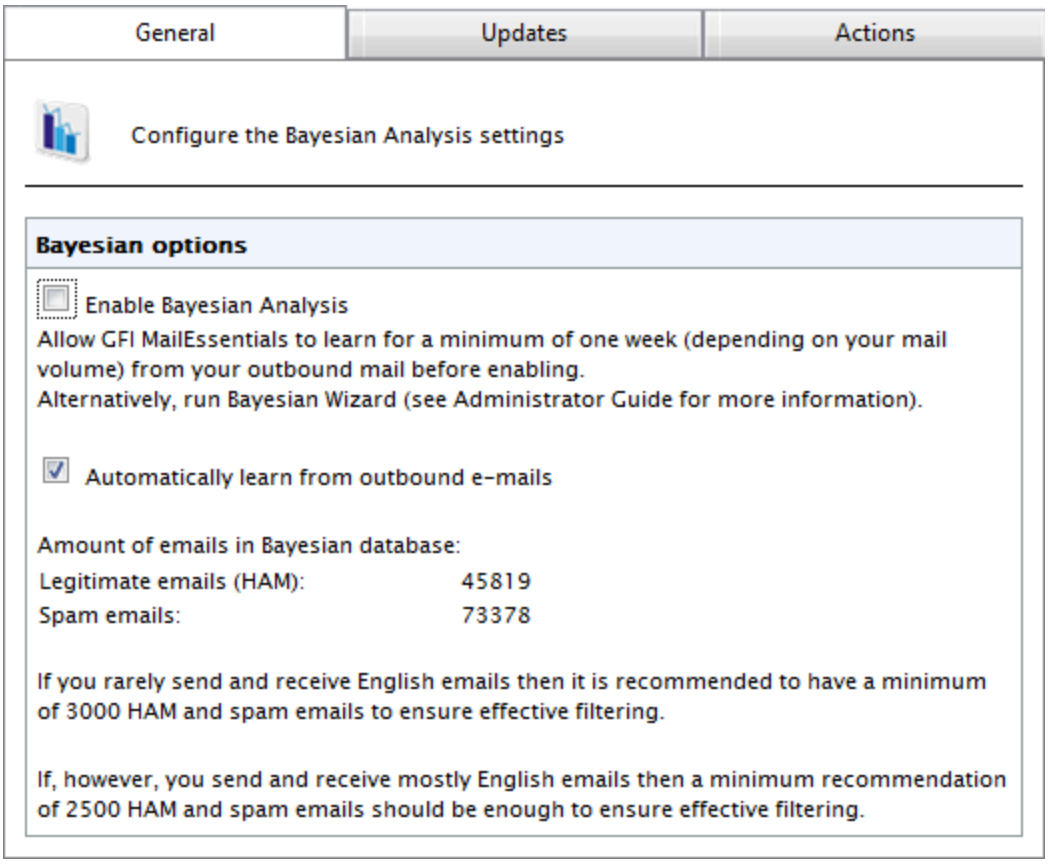
GFI Anti-Spam Folders public folders trains the Bayesian filter in the same way as live outbound email sending.

> **NOTE**
>
> To use this option, Public Folder Scanning must be enabled. For more information, refer to Public Folder Scanning (page 149).

Stage 2: Enabling the Bayesian filter

After the Bayesian filter is trained, it must be enabled.

1. From GFI MailEssentials configuration console, go to **Anti-Spam > Anti-Spam Filters > Bayesian Analysis**.
2. From the **General** tab select **Enable Bayesian Analysis**.


General
Updates
Actions
Configure the Bayesian Analysis settings
Bayesian options
Enable Bayesian Analysis
Allow GFI MailEssentials to learn for a minimum of one week (depending on your mail volume) from your outbound mail before enabling.
Alternatively, run Bayesian Wizard (see Administrator Guide for more information).
Automatically learn from outbound e-mails
Amount of emails in Bayesian database:
Legitimate emails (HAM): 45819
Spam emails: 73378
If you rarely send and receive English emails then it is recommended to have a minimum of 3000 HAM and spam emails to ensure effective filtering.
If, however, you send and receive mostly English emails then a minimum recommendation of 2500 HAM and spam emails should be enough to ensure effective filtering.

Screenshot 69: Bayesian analysis properties

3. In the **Updates** tab, configure the frequency of updates to the spam database by enabling **Automatically check for updates** and configuring an hourly interval.

> **NOTE**
>
> Click **Download updates now** to immediately download any updates.

NOTE

You can download updates using a proxy server. For more information, refer to Proxy settings (page 221).

4. Click **Actions** tab to select the actions to perform on messages identified as spam. For more information, refer to Spam Actions - What to do with spam emails (page 135).
5. Click **Apply**.

NOTE

GFI MailEssentials also provides a Bayesian Analysis wizard that enables you to train the Bayesian Analysis filter from a machine other than where GFI MailEssentials is installed. For more information, refer to Training the Bayesian Analysis filter (page 266).

7.1.13 Whitelist

NOTE

Whitelist affects only Anti-Spam filters and not email security and content filtering

The Whitelist contains lists of criteria that identify legitimate email. Emails that match these criteria are not scanned by anti-spam filters and are always delivered to the recipient. Emails can be whitelisted using the following criteria:

- Sender's email address, email domain or IP address
- Senders to whom an email was previously sent (Auto-whitelist)
- Recipient (exclude local email addresses from having emails filtered)
- Keywords in email body or subject

The whitelist and autowhitelist features are enabled by default.

Important notes

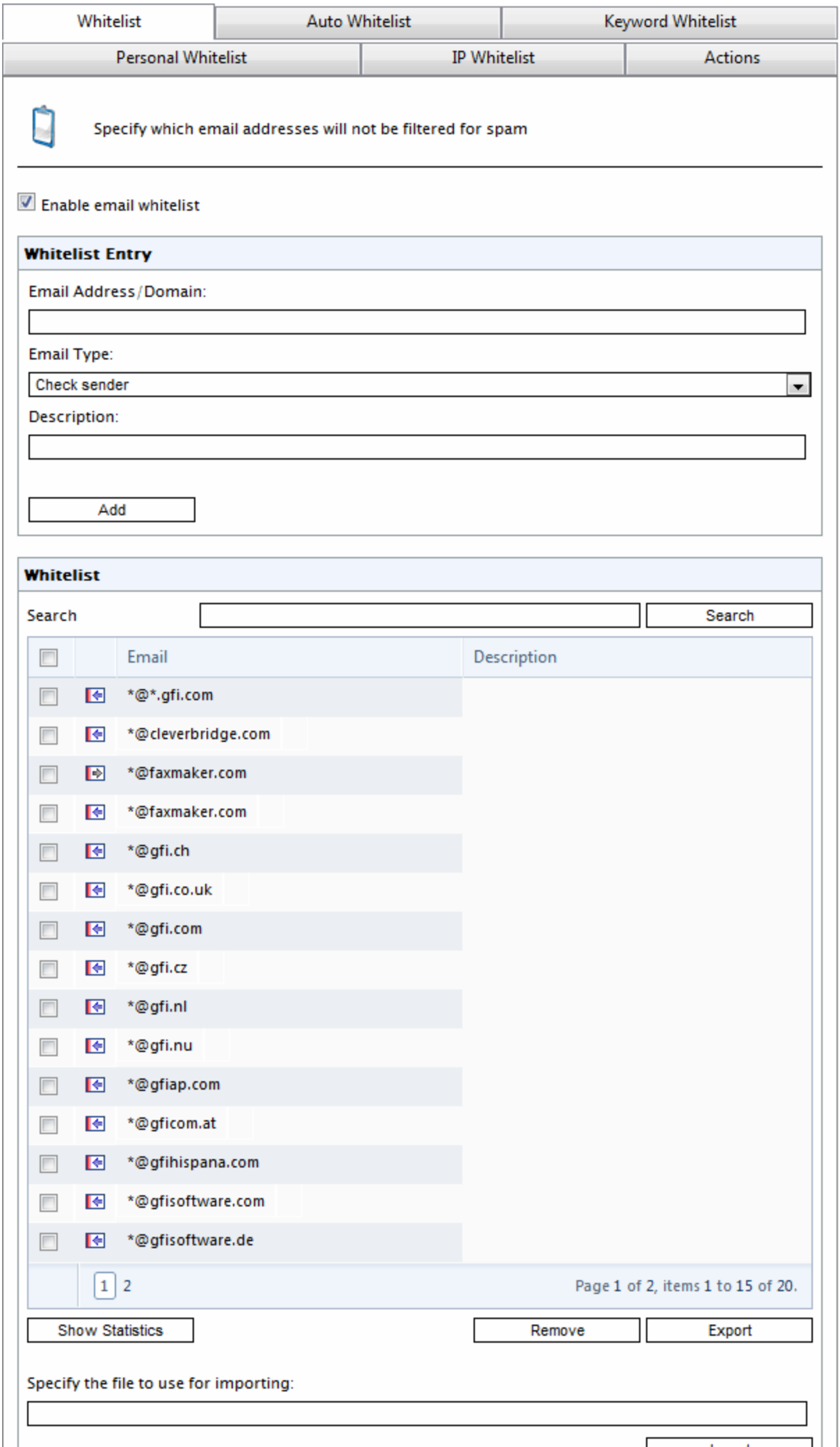
Using the autowhitelist feature is highly recommended since this eliminates a high percentage of false positives.

In Keyword Whitelist it is recommended to add terms that spammers do not use and terms that relate to your nature of business, for example your product names. Entering too many keywords increases the possibility of emails not filtered by GFI MailEssentials and delivered to users' mailboxes.

Whitelisting an internal user defeats the purpose of the Anti-Spoofing filter. For more information, refer to Anti-Spoofing (page 117).

Configuring Whitelist

1. Go to **Anti-Spam > Whitelist**.


Whitelist
Auto Whitelist
Keyword Whitelist
Personal Whitelist
IP Whitelist
Actions
Specify which email addresses will not be filtered for spam
Enable email whitelist
Whitelist Entry
Email Address/Domain:
Email Type:
Check sender
Description:
Add
Whitelist
Search
Search
Email
Description
@.gfi.com
*@cleverbridge.com
*@faxmaker.com
*@faxmaker.com
*@gfi.ch
*@gfi.co.uk
*@gfi.com
*@gfi.cz
*@gfi.nl
*@gfi.nu
*@gfiap.com
*@gficom.at
*@gfihispana.com
*@gfisoftware.com
*@gfisoftware.de
1 2
Page 1 of 2, items 1 to 15 of 20.
Show Statistics
Remove
Export
Specify the file to use for importing:

Screenshot 70: Whitelist tab

2. From the **Whitelist** tab, configure the email addresses and domains to whitelist. Select/Unselect **Enable email whitelist** to enable/disable whitelist. Perform the following actions:

Action	Description
Add a whitelist entry	1. In **Email Address/Domain**, provide the email address/domain to whitelist. **For example:** . *@companysupport.com or. *@*.edu. 2. In **Email Type** specify the email header field to match for the emails to be whitelisted. **NOTE** For more information about the difference between SMTP and MIME refer to: http://go.gfi.com/?pageid=ME_DifferenceSMTPMIME 3. (Optional) In **Description** add a description to the entry. 4. Click **Add**.
Remove whitelist entries	1. Select one or more whitelist entries from the **Whitelist** list. 2. Click **Remove**.
Search for a whitelist entry	1. In **Search**, key in the details of the whitelist entry to search for. 2. Click **Search** to display list of matching terms.
Show Statistics	Use the **Show Statistics** button to view the total number of emails blocked per whitelist entry.
Import whitelist entries	1. Specify the full path and filename of the file to use for importing the previously exported data. 2. Click **Import** to import entries.
Export whitelist entries	Click **Export** to export current list of whitelist entry to an XML file.

3. Select the **Auto Whitelist** tab to configure the following options:

Option	Description
Populate Auto Whitelist automatically:	If selected, destination email addresses of outbound emails are automatically added to the auto-whitelist.
Enable Email Auto Whitelist	Select this option to enable auto-whitelist. Senders of incoming emails are matched against the auto-whitelist. If the sender is present in the list, the email is forwarded directly to the recipient's Inbox.
Maximum entries allowed in the Auto Whitelist:	Specify the number entries allowed in Auto-Whitelist. When the limit specified is exceeded, the oldest and least used entries are automatically replaced by the new entries. **NOTE** Entering a value larger than the default value of 30,000 can negatively affect the performance of GFI MailEssentials.

4. From the **Keyword Whitelist** tab, specify keywords that flag emails as valid emails:

Option	Description
Enable email body keyword whitelist	Select this option to check for keywords in the email body which qualify an email as valid. Add keywords to the **Body Keywords** list. You can also import or export lists of keywords from/to an XML file.
Enable email subject keyword whitelist	Select this option to check for keywords in the email subject which qualify an email as valid. Add keywords to the **Subject Keywords** list. You can also import or export lists of keywords from/to an XML file.
Match whole words only (words/phrases in subject/body)	When selecting this option, only whole words from the keyword whitelist are matched that qualify an email as valid.

5. From the **IP Whitelist** tab, configure:

Option	Description
Enable IP Whitelist	Select to allow emails received from specific IP addresses to be whitelisted.
Add IP Whitelist entries	1. Specify: » **Single computer / CIDR**: Key in a single IP address or a range of IP addresses using CIDR notation. » **Group of computers**: Specify the **Subnet Address** and **Subnet Mask** of the group of IPs to whitelist. 2. (Optional) Add a **Description**. 3 Click **Add**.
Remove IP Whitelist entries	Select the IPs to remove and click **Remove**.

6. Click **Actions** tab to enable / disable logging of whitelist occurrences to a file. Provide a path/folder where to store the generated log file.
7. Click **Apply**.

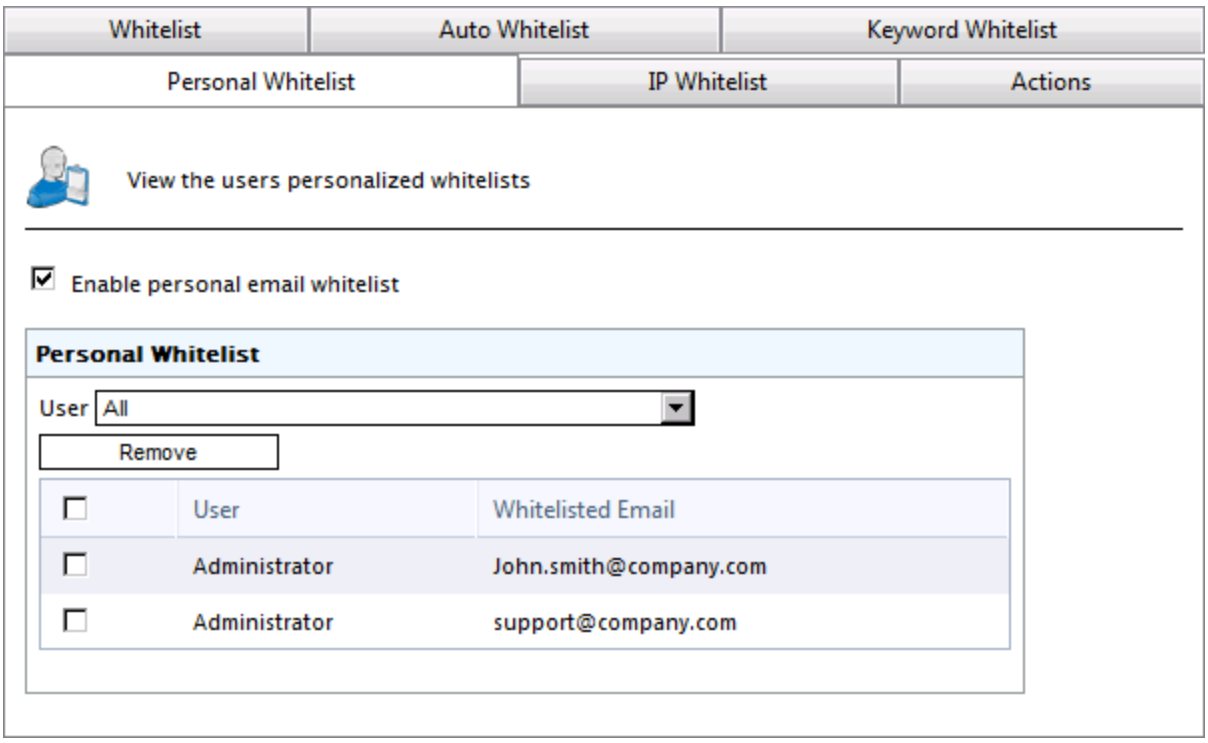
Personal Whitelist

The personal whitelist is an additional whitelist that compliments global whitelist. Disabled by default, the personal whitelist can be enabled for users allowing them to add specific email addresses to a personal whitelist that they can manage. For more information, refer to Personal Whitelist and Blocklist (page 62).

For management purposes, administrators can also remove specific email addresses that the users have added to their personal whitelist.

Enabling/Disabling Personal Whitelists

1. Go to **Anti-Spam > Whitelist**.



Screenshot 71: Personal whitelist

2. Select **Personal Whitelist** tab and select or unselect **Enable personal email whitelist** to enable or disable personal whitelist feature.
3. Click **Apply**.

Removing emails from users' personal whitelist

1. Go to **Anti-Spam > Whitelist** and select **Personal Whitelist** tab.
2. From the **User** drop down list, select the user for whom to delete an email address.
3. Select an email address from the list of email addresses. Click **Remove**.
4. Click **Apply**.

7.1.14 New Senders

The New Senders filter identifies emails that have been received from senders to whom emails have never been sent before. Such senders are identified by referencing the data collected in the Whitelist.

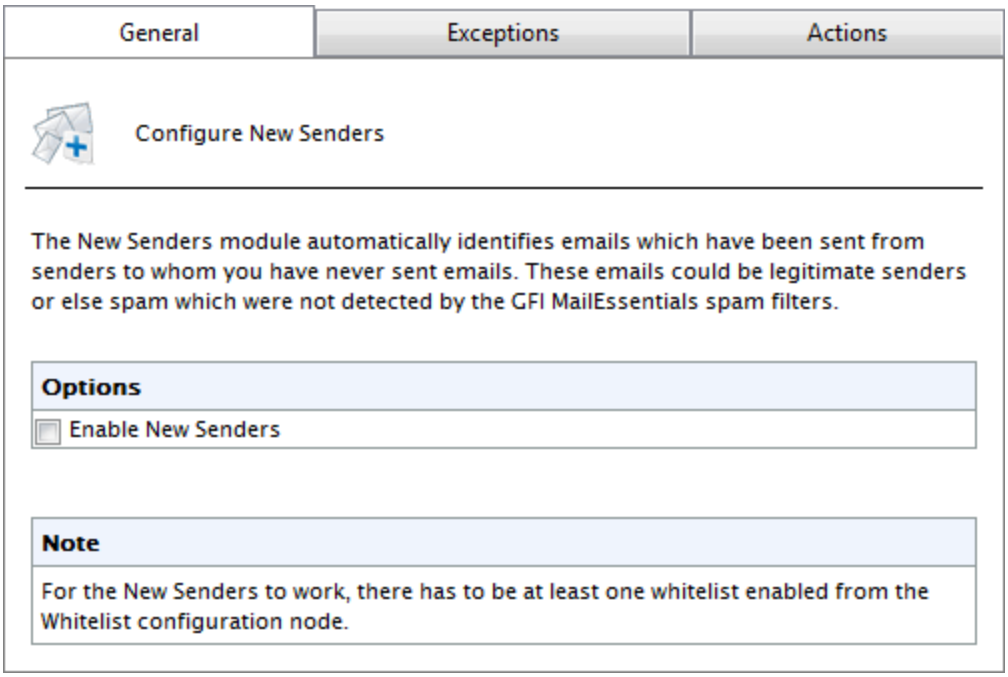
Only emails in which no spam is detected and where the sender is not present in any Whitelist are triggered by the New Senders filter.

This filter is **NOT** enabled by default.

> **Important**
>
> Enable at least one of the available Whitelists to use the New Senders function. In the absence of the Whitelist functions (should no spam be detected by the other filters) received messages will be delivered to the recipient's Inbox. **ONLY** emails in which no spam was detected and whose senders are not present in the Whitelist are delivered in the New Senders folder.

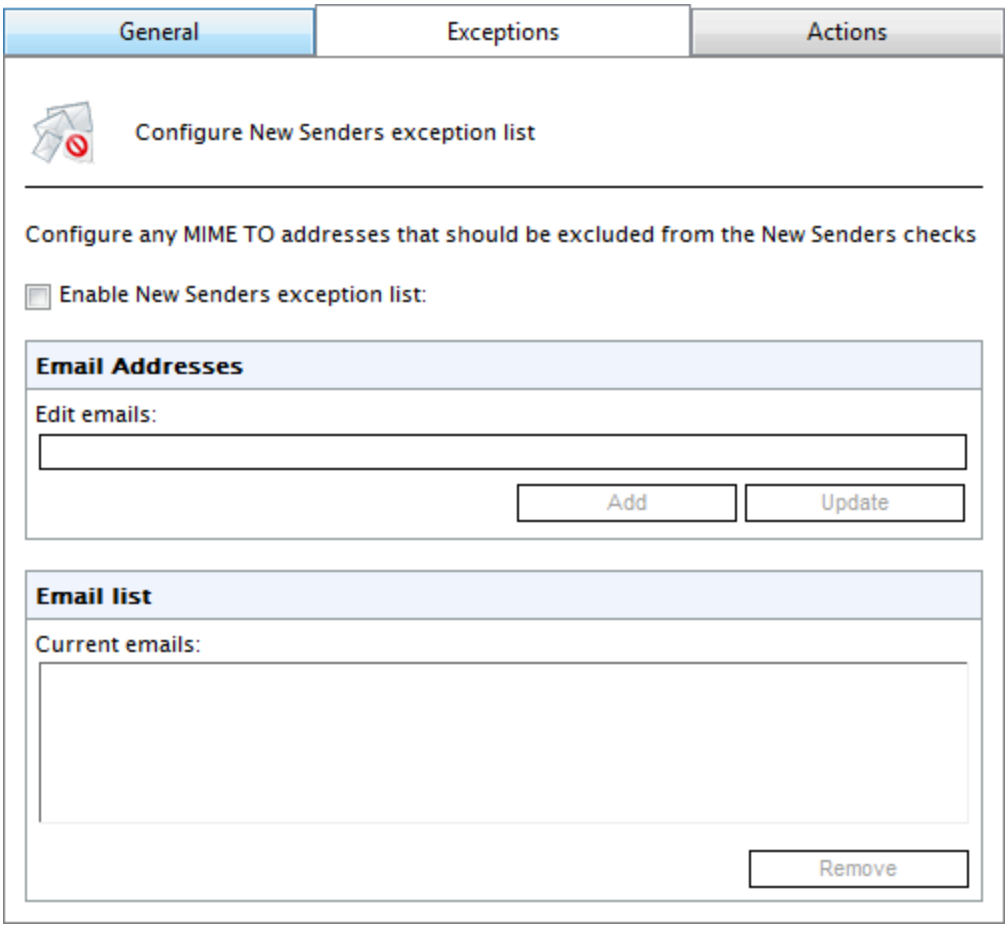
Configuring New Senders Filter

1. Go to **Anti-Spam > New Senders**.


General
Exceptions
Actions
Configure New Senders
The New Senders module automatically identifies emails which have been sent from senders to whom you have never sent emails. These emails could be legitimate senders or else spam which were not detected by the GFI MailEssentials spam filters.
Options
Enable New Senders
Note
For the New Senders to work, there has to be at least one whitelist enabled from the Whitelist configuration node.

Screenshot 72: New Senders General tab

2. In the **General** tab, select **Enable New Senders** to enable check for new senders on all inbound messages.



Screenshot 73: New Senders Exceptions

3. From **Exceptions** tab, configure senders/recipients whose emails are excluded from the New Senders check.

Option	Description
Enable New Senders exception list	Select this option to enable the exceptions list.
Add exception	Key in an email address to exclude and click **Add**. Repeat for each address to add.
Edit exception	1. Select an exception from the **Email list**. 2. Edit the email address. 3. Click **Update**.
Delete exception	Select an exception from the **Email list** and click **Remove**.

4. Click **Actions** tab to select the actions to perform on messages identified as spam. For more information, refer to Spam Actions - What to do with spam emails (page 135).

5. Click **Apply**.

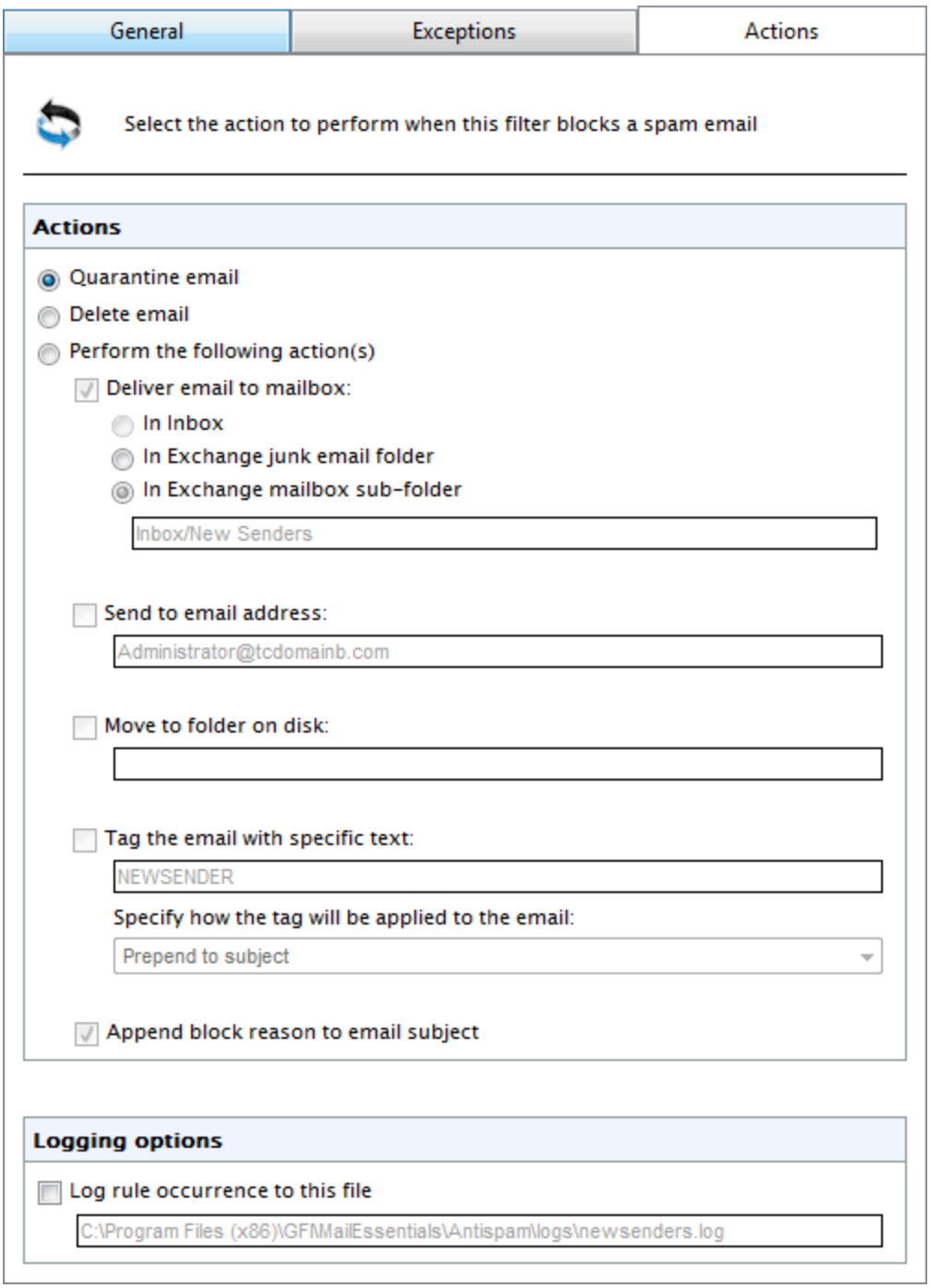
7.2 Spam Actions - What to do with spam emails

The **Actions** tab in the Anti-Spam filters properties define what should be done with emails marked as spam. Different actions can be defined for each of the spam filters.

» **For Example:** Delete emails detected by SpamRazer filter, but do not delete emails marked as spam by the Email Blocklist filter.

7.2.1 Configuring Spam Actions

In the **Actions** tab, select an option that defines which action to take on emails marked as spam.



Screenshot 74: Anti-spam actions

Action	Description
Quarantine Email	Emails detected as spam are stored in the Quarantine Store. Other spam actions are disabled if the email is quarantined. For more information, refer to Quarantine (page 180).
Delete Email	Delete an email blocked by that particular spam filter. Other spam actions are disabled if the email is deleted.

Action	Description
Deliver email to mailbox	Choose the folder where to deliver the email. Available options are: » **In Inbox** - Routes spam to user's inbox » **In Exchange junk email folder** - Routes spam to users's default junk email folder. **NOTE** The **In Exchange junk email folder** option is not available when configuring the New Senders filter. » **In Exchange mailbox sub-folder** - Route all spam to a specific folder in the user's mailbox. Type the folder where to move spam email. • **Example 1:** Type `Suspected Spam` for a custom folder to be created in the same level of the Inbox folder. • **Example 2:** Type `Inbox\Suspected Spam` for a custom folder to be created in the Inbox folder. **NOTE** This option requires that: » GFI MailEssentials is installed on the Microsoft® Exchange Server machine. If GFI MailEssentials is not installed on the Microsoft® Exchange Server, configure mail server to route emails or use the Rules Manager. For more information, refer to Moving spam email to user's mailbox folders (page 238). » The mail server is Microsoft® Exchange Server 2003 or Microsoft® Exchange Server 2007/2010 with the Mailbox Server Role present. **NOTE** For Microsoft® Exchange 2010 a dedicated user is required to enable this option. For more information, refer to Move spam to Exchange 2010 folder (page 240).
Send to email address	Send email identified as spam to a specific email address. **Example:** Forward all spam to an email address checked by someone who checks email that might have been wrongly marked as spam. The subject of the email will be in the format: `[recipient] [subject]`
Move to folder on disk	Saves email detected as spam to the path specified, **Example:** `C:\Spam\` File names of saved emails are in the following format: `[Sender_recipient_subject_number_.eml]` **Example:** `C:\Spam\jim@comp.com_bob@comp.com_MailOffers_1_.eml`)

Action	Description
Tag the email with specific text	Select this option to add a tag to the email subject. Key in the text to use for tagging and specify where to place the tag: » **Prepend to subject** - insert the specified tag at the start (i.e. as a prefix) of the email subject text. **Example:** `[SPAM]Free Web Mail` » **Append to subject -** insert the specified tag at the end (i.e. as a suffix) of the email subject text. **Example:** `Free Web Mail[SPAM]` » **Add tag in an X-header…** - Add the specified tag as a new X-header to the email. In this case, the X-Header will have the following format : • `X-GFIME-SPAM: [TAG TEXT]` • `X-GFIME-SPAM-REASON: [REASON]` **Example:** – `X-GFIME-SPAM: [This is SPAM]` – `X-GFIME-SPAM-REASON: [IP DNS Blocklist Check failed - Sent from Blocklisted Domain]` **NOTE** Rules manager can be used to move emails when this feature is used.
Append block reason to email subject	If this option is enabled, the name of the filter which blocked the email and the reason for blocking are appended to the subject of the blocked email.
Log rule occurrence to this file	Log the spam email occurrence to a log file of your choice. By default, log files are stored in: *<GFI MailEssentials installation path>*\GFI\MailEssentials\AntiSpam\Logs\<filtername>.log **NOTE** Log files may become very large. GFI MailEssentials enables log rotation, where new log files are created periodically or when the log file reaches a specific size. To enable log file rotation navigate to **Anti-Spam > Anti-Spam Settings**. Select **Anti-spam logging** tab and check **Enable log file** rotation. Specify the rotation condition by time or file size.

7.3 Sorting anti-spam filters by priority

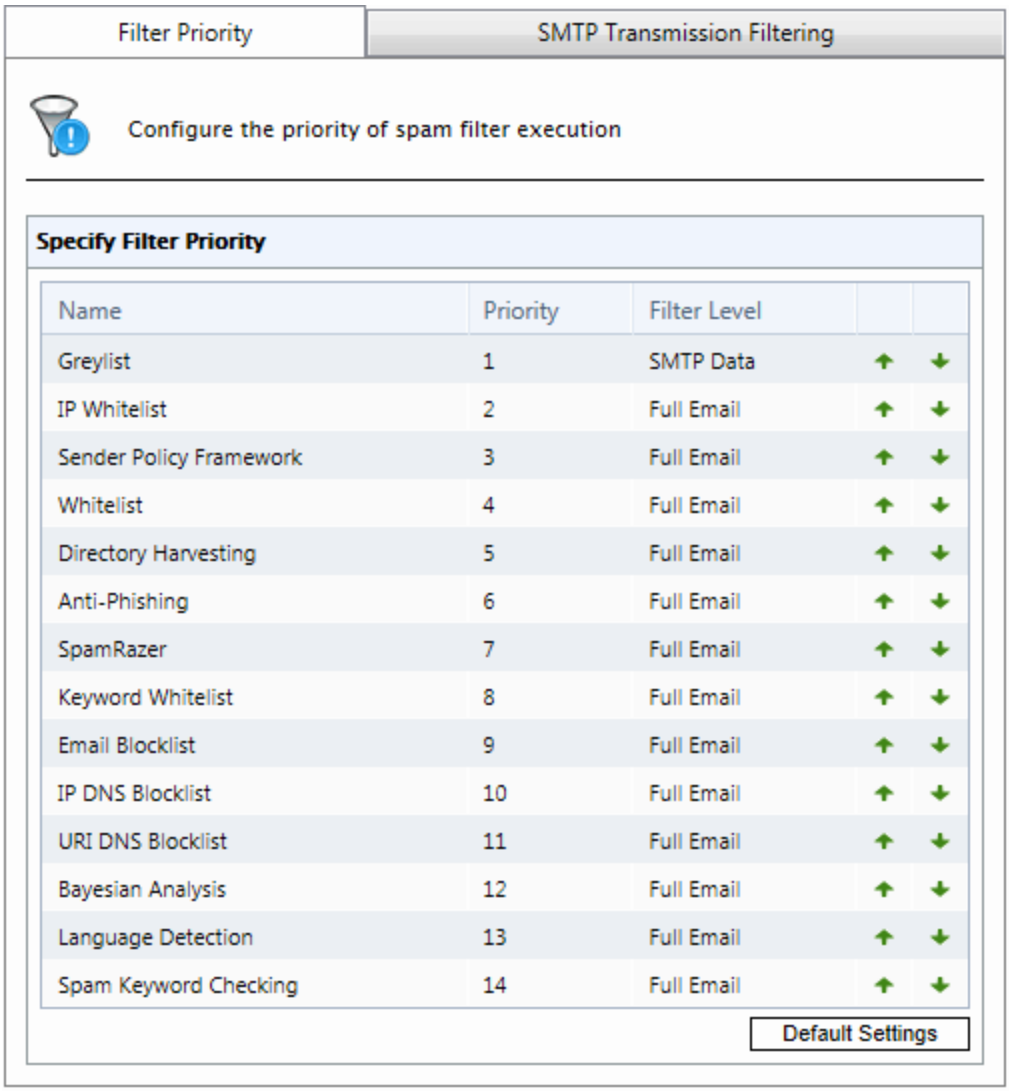
In GFI MailEssentials, the order in which the anti-spam checks are applied to inbound messages can be customized.

NOTE

The order of all available filters can be customized except for the New Senders filter, which is always automatically set to the lowest priority. This is due to its dependency on the results of the Whitelist checks and the other anti-spam filters.

Default priority is recommended in most situations.

1. Go to **Anti-Spam > Filter Priority**.


Filter Priority
SMTP Transmission Filtering
Configure the priority of spam filter execution
Specify Filter Priority
Name
Priority
Filter Level
Greylist 1 SMTP Data
IP Whitelist 2 Full Email
Sender Policy Framework 3 Full Email
Whitelist 4 Full Email
Directory Harvesting 5 Full Email
Anti-Phishing 6 Full Email
SpamRazer 7 Full Email
Keyword Whitelist 8 Full Email
Email Blocklist 9 Full Email
IP DNS Blocklist 10 Full Email
URI DNS Blocklist 11 Full Email
Bayesian Analysis 12 Full Email
Language Detection 13 Full Email
Spam Keyword Checking 14 Full Email
Default Settings

Screenshot 75: Assigning filter priorities

2. Select a filter and click (up) button to assign a higher priority or click (down) button to assign a lower priority.

> **NOTE**
>
> Click **Default Settings** to restore the filters' order to default.

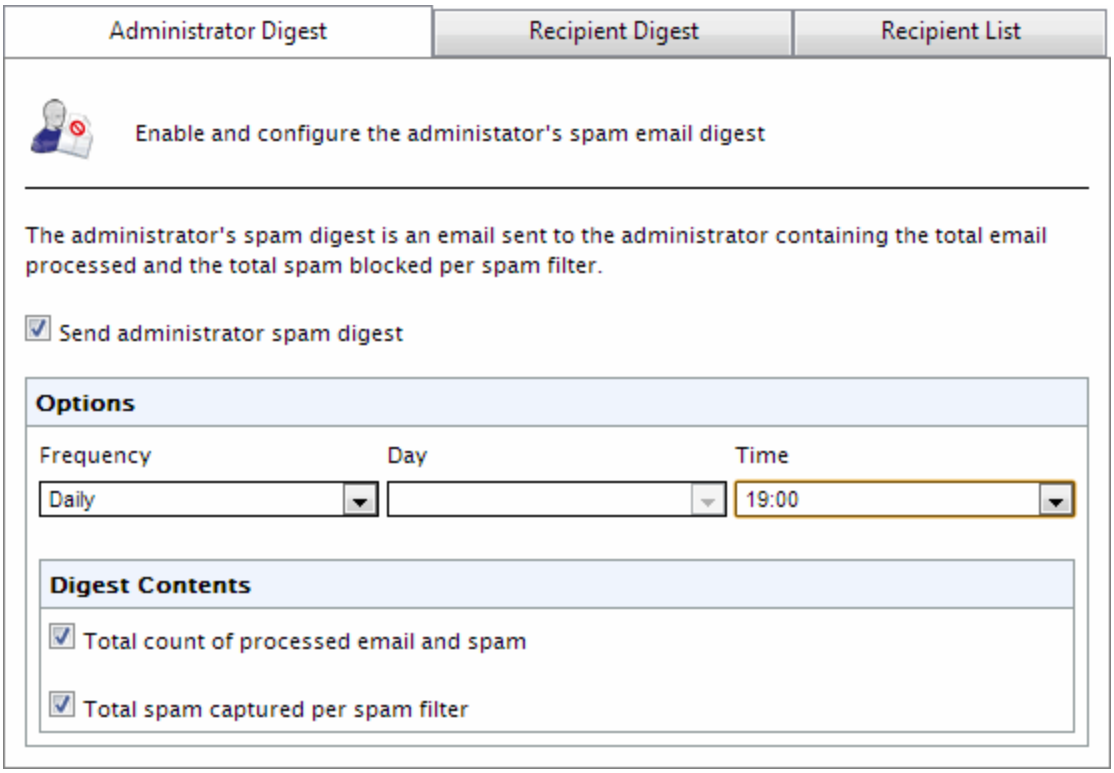
3. Click **Apply**.

7.4 Spam Digest

The spam digest is a short report sent to an administrator or user via email. This report lists the total number of emails processed by GFI MailEssentials and the number of spam emails blocked over a specific period of time (since the last spam digest).

7.4.1 Configuring spam digests - Administrator spam digest

1. Go to **Anti-Spam > Spam Digest**.

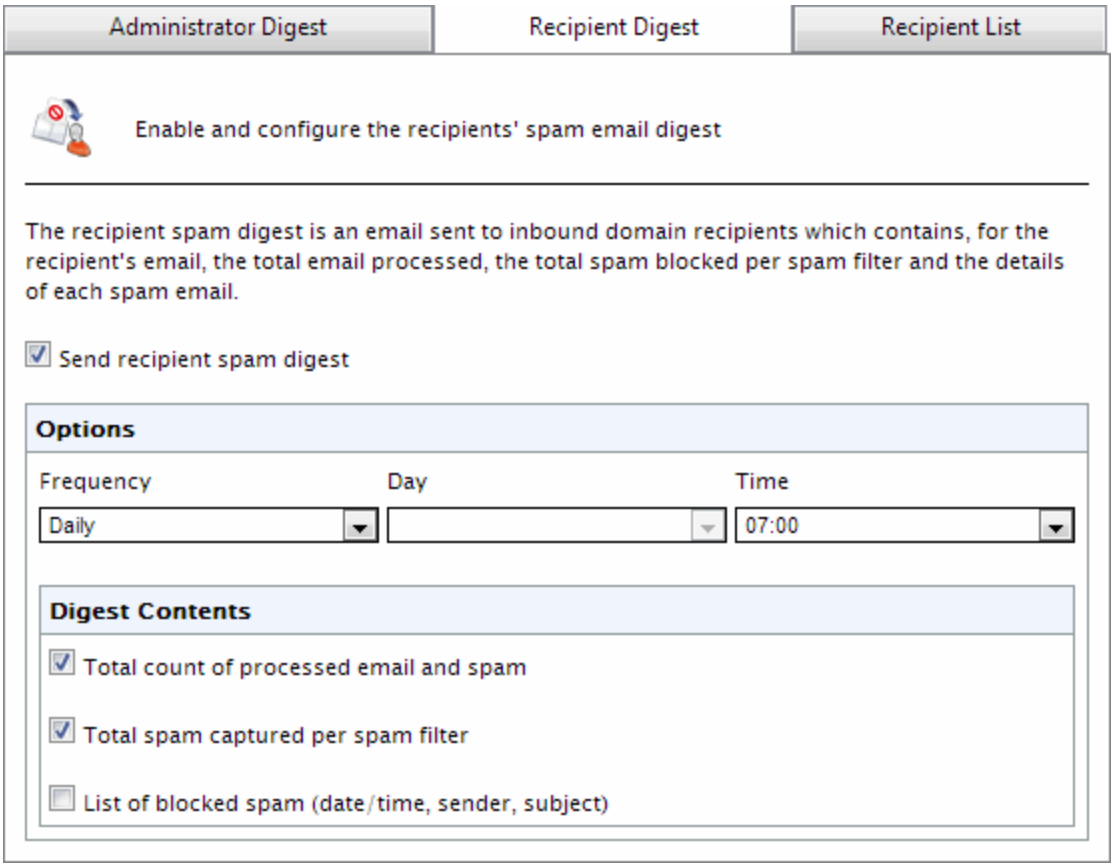

Administrator Digest
Recipient Digest
Recipient List
Enable and configure the administator's spam email digest
The administrator's spam digest is an email sent to the administrator containing the total email processed and the total spam blocked per spam filter.
Send administrator spam digest
Options
Frequency
Day
Time
Daily
19:00
Digest Contents
Total count of processed email and spam
Total spam captured per spam filter

Screenshot 76: Spam digest properties/ Administrator spam digest

2. From the **Administrator Digest** tab, click **Send administrator spam digest** to enable spam digest.
3. Configure the desired sending frequency (Daily, Weekly, Monthly) and specify a date and a time when email is sent.
4. Specify the digest content that will be sent in the email, either a **Total count of processed email and spam** or **Total spam captured per spam filter** or both.
5. Finalize settings by selecting **Apply**.

7.4.2 Configuring spam digests - Recipient spam digest

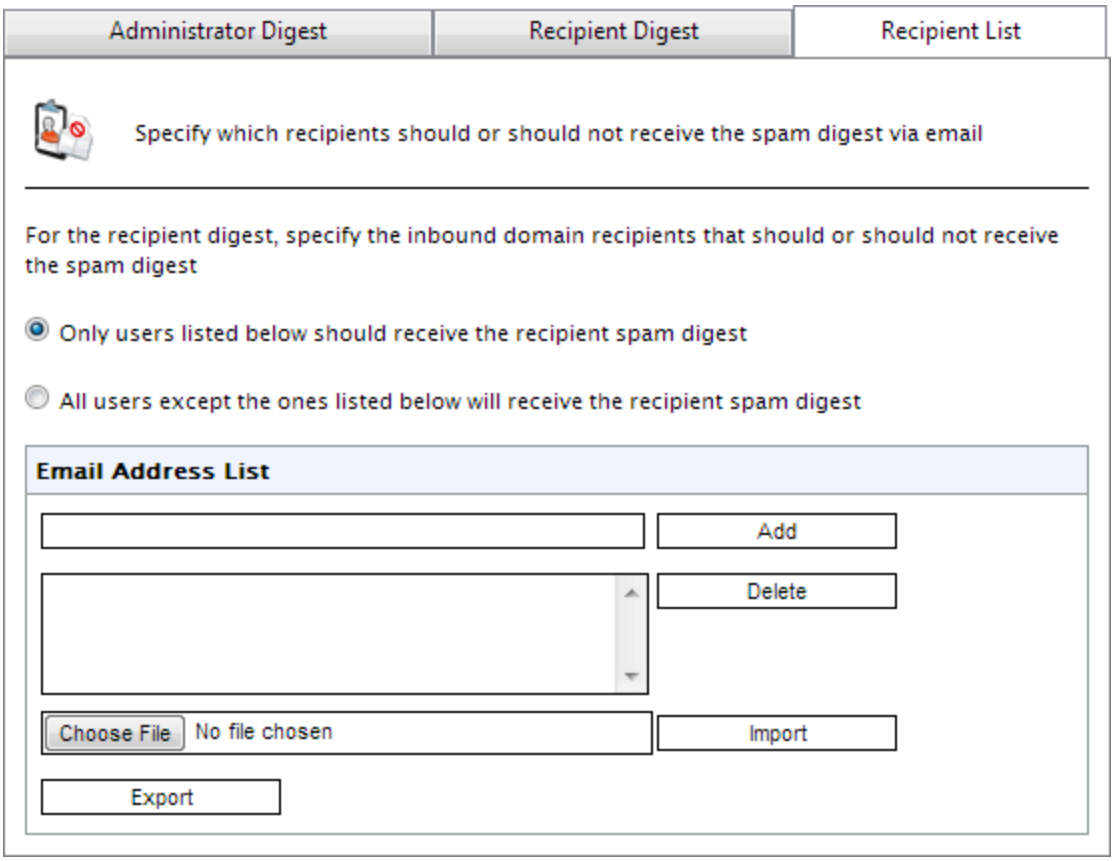
1. Go to **Anti-Spam > Spam Digest**.


Administrator Digest
Recipient Digest
Recipient List
Enable and configure the recipients' spam email digest
The recipient spam digest is an email sent to inbound domain recipients which contains, for the recipient's email, the total email processed, the total spam blocked per spam filter and the details of each spam email.
Send recipient spam digest
Options
Frequency
Day
Time
Daily
07:00
Digest Contents
Total count of processed email and spam
Total spam captured per spam filter
List of blocked spam (date/time, sender, subject)

Screenshot 77: Recipient spam digest

2. From the **Recipient Digest** tab, select **Send recipient spam digest** to enable spam digest.
3. Configure the desired sending frequency (Daily, Weekly, Monthly) and specify a date and a time when email is sent.
4. Specify the digest content that will be sent in the email:

- Total count of processed email and spam
- Total spam captured per spam filter
- List of blocked spam or any combination of options as required.


Administrator Digest
Recipient Digest
Recipient List
Specify which recipients should or should not receive the spam digest via email
For the recipient digest, specify the inbound domain recipients that should or should not receive the spam digest
Only users listed below should receive the recipient spam digest
All users except the ones listed below will receive the recipient spam digest
Email Address List
Add
Delete
Choose File
No file chosen
Import
Export

Screenshot 78: Spam digest recipient list

4. Click on the **Recipients list** tab, add the users to receive the spam digest and select the method used to determine who should receive the spam digest.

Available options are:

- Only users listed below should receive the recipient spam digest.
- All users except the ones listed below will receive the recipient spam digest.

> **NOTE**
>
> The required list of users can also be imported from a file in XML format in the same structure that GFI MailEssentials would export files.

6. Select **Apply** to finalize settings.

7.5 Anti-Spam settings

The following settings are configurable for anti-spam filters and emails blocked by anti-spam filters only.

7.5.1 Log file rotation 143

7.5.2 Anti-Spam Global Actions 143

7.5.3 DNS Server Settings 144

7.5.4 Remote Commands 145

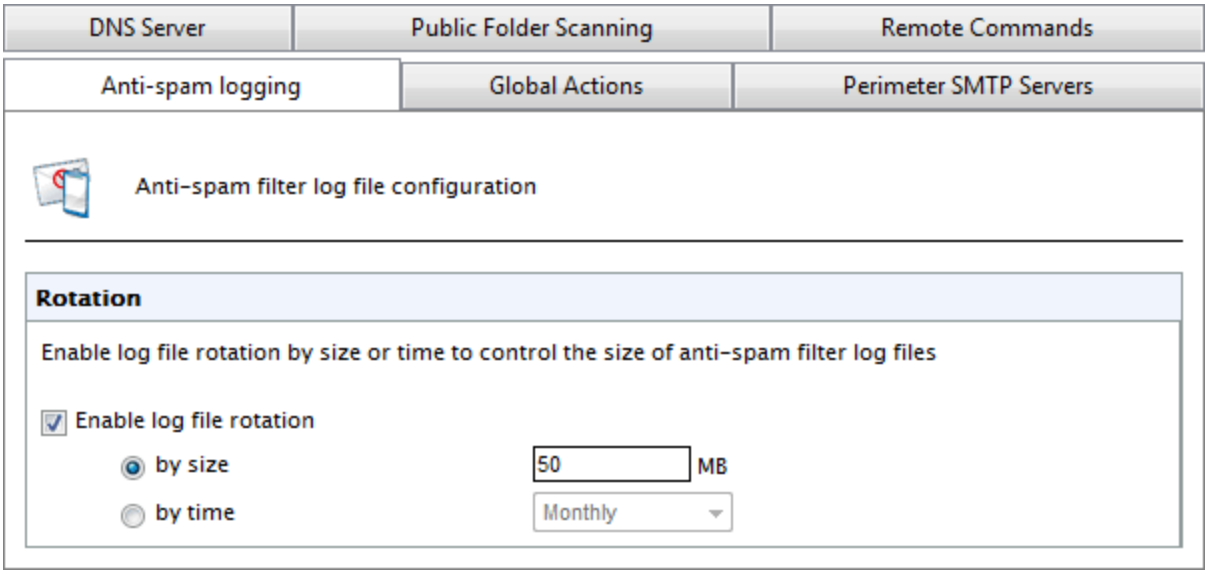
7.5.5 Perimeter SMTP Server Settings 148

7.5.1 Log file rotation

Over time, log files may become very large. GFI MailEssentials enables log rotation, where new log files are created periodically or when the log file reaches a specific size.

To enable log file rotation:

1. Go to **Anti-Spam** > **Anti-Spam Settings**.



Screenshot 79: Log file rotation

2. From the **Anti-spam logging** tab, select **Enable log file rotation** and specify the rotation condition (**by size** or **by time**).
3. Provide the size or time values and click **Apply**.

7.5.2 Anti-Spam Global Actions

A lot of spam is sent to email addresses that no longer exist. Generally, these emails are simply deleted however for troubleshooting or evaluation purposes, you might want to move these emails to a folder or forward them to a particular email address.

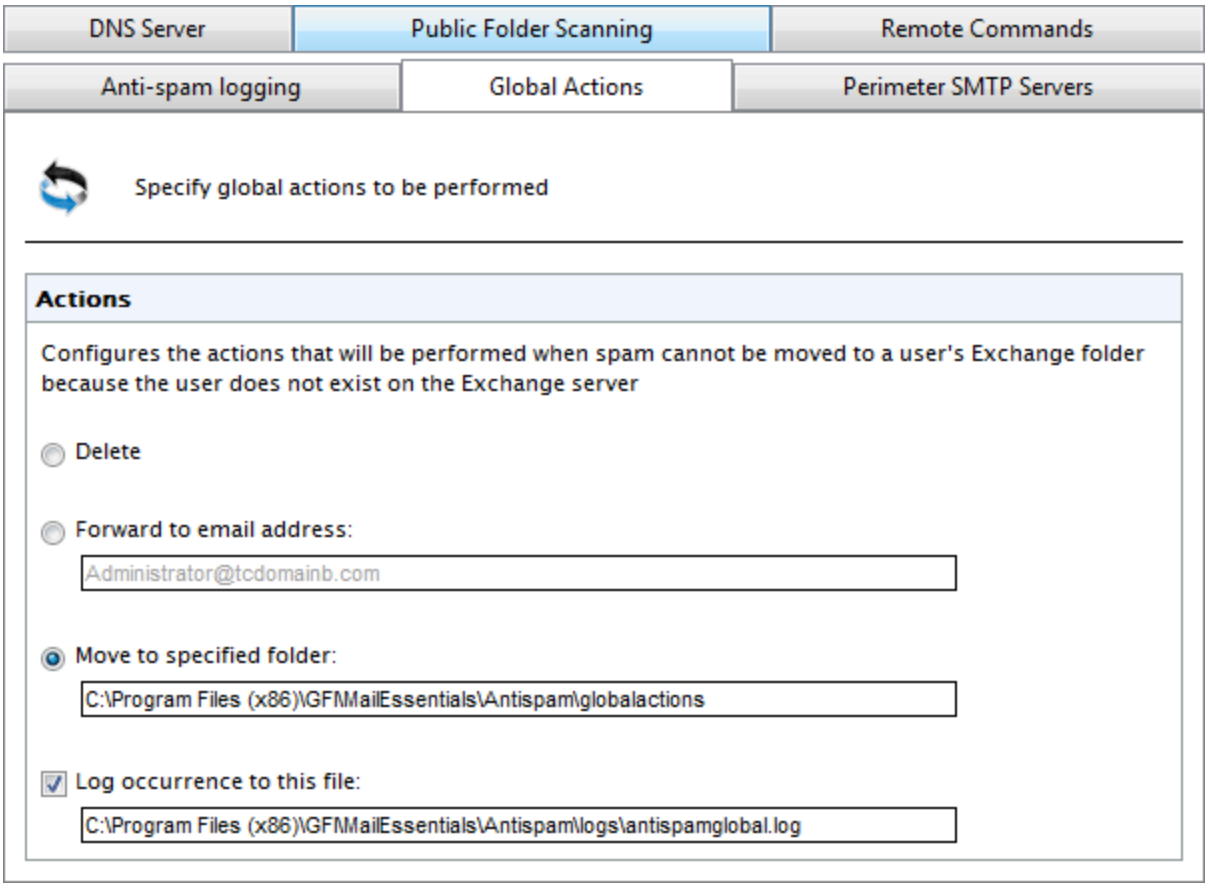
NOTE

This section only applies for installations on Microsoft® Exchange Server that have spam action **Move to subfolder of user's mailbox** enabled. For more information, refer to Spam Actions - What to do with spam emails (page 135).

On other mail servers, the anti-spam global actions tab will not appear.

Configuring Anti-spam global actions

1. Go to **Anti-Spam** > **Anti-Spam Settings**.


DNS Server
Public Folder Scanning
Remote Commands
Anti-spam logging
Global Actions
Perimeter SMTP Servers
Specify global actions to be performed
Actions
Configures the actions that will be performed when spam cannot be moved to a user's Exchange folder because the user does not exist on the Exchange server
Delete
Forward to email address:
Administrator@tcdomainb.com
Move to specified folder:
C:\Program Files (x86)\GFIMailEssentials\Antispam\globalactions
Log occurrence to this file:
C:\Program Files (x86)\GFIMailEssentials\Antispam\logs\antispamglobal.log

Screenshot 80: Global actions

2. Select **Global Actions** tab and choose whether to:

» Delete the email

» Forward it to an email address

» Move it to a specified folder.

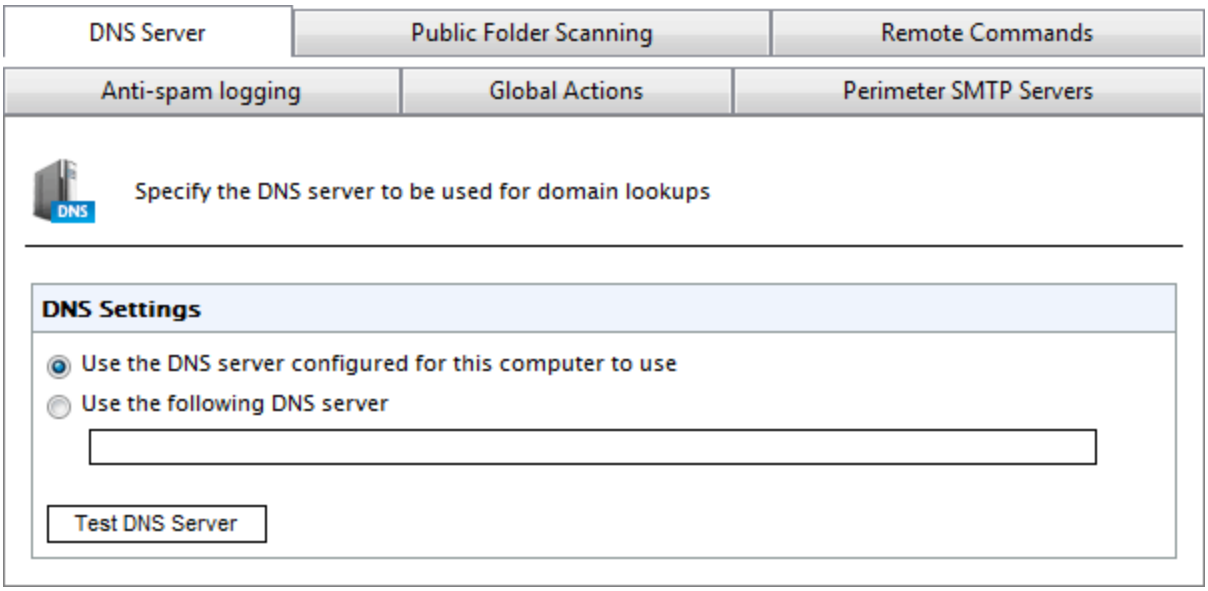
3. Select **Log occurrence to this file** to log these occurrences to a log file.

4. Click **Apply**.

7.5.3 DNS Server Settings

DNS Server settings are very important in GFI MailEssentials since a number of anti-spam filters, such as IP DNS Blocklist, URI DNS Blocklist and SpamRazer, perform domain lookups when filtering spam.

1. From the GFI MailEssentials Configuration, go to **Anti-Spam > Anti-Spam Settings**.


DNS Server
Public Folder Scanning
Remote Commands
Anti-spam logging
Global Actions
Perimeter SMTP Servers
Specify the DNS server to be used for domain lookups
DNS Settings
Use the DNS server configured for this computer to use
Use the following DNS server
Test DNS Server

Screenshot 81: DNS server settings

1. From the **DNS Server** tab configure:

Option	Description
Use the DNS server configured for this computer to use	Select this option to use the same DNS server that is used by the operating system where GFI MailEssentials is installed.
Use the following DNS server	Select this option to specify a DNS server that is different than the one used by the local machine.

2. Click **Test DNS Server** to test connectivity with the specified DNS server. If unsuccessful, specify another DNS server.
3. Click **Apply**.

7.5.4 Remote Commands

Remote commands facilitate adding domains or email addresses to the Email Blocklist/Whitelist, as well as update the Bayesian filter with spam or ham (valid emails).

Remote commands work by sending an email to GFI MailEssentials. Addressing an email to **rcommands@mailessentials.com** (configurable) will have GFI MailEssentials recognize the email as containing remote commands and processes them as described below.

With remote commands, the following tasks can be achieved:

1. Add Spam or ham to the Bayesian Analysis database.
2. Add keywords either to the subject keyword checking feature or to the body keyword checking feature.
3. Add email addresses to the Email Blocklist filter and Whitelist.

Configuring remote commands

1. Click **Anti-Spam > Anti-Spam Settings**, go to **Remote Commands** tab and select **Enable remote commands**.

2. Edit the email address to which remote commands should be sent to.

NOTE

The email address should **NOT** be a local domain. The default address is **rcommands@mailessentials.com**. A mailbox for the configured address does not need to exist, but the domain-part of the address must consist of a real email address domain that returns a positive result to an MX-record lookup via DNS. This can also be a public email account that you can manage (for example gmail or yahoo mail)

3. Optionally, configure some basic security for remote commands:
   - A shared password to include in the email. For more information, refer to Using remote commands (page 146).
   - Which users are allowed to send emails with remote commands.
4. Click **Apply**.

Using remote commands

Remote commands can be sent via email to GFI MailEssentials from an email client within the domain. Conditions for sending remote commands:

- The email must be in Plain Text format
- The subject of the email is ignored
- The following syntax must be used for all commands:

  `<command name>: <parameter1>, <parameter2>, <parameter3>, … ;`

  For example: `ADDBLIST: spammer@spam.com;`
- There can be more than one command in the body of an email with each command separated by a semi-colon (;).
- If a password is configured for remote commands, enter the password in the first line using the following syntax:

  `PASSWORD: <shared password>;`
- Command names are case-sensitive and should be written in UPPERCASE only.
- Conditions such as `IF, AND, OR` are not supported.
- Remote commands can only be used to add entries and not delete or modify existing entries.

Keyword commands

Use keyword commands to add keywords or combination of keywords in the body or subject lists in Keyword Checking filter.

Available commands are:

- ADDSUBJECT - Adds keywords specified to the subject keyword checking database.
  - Example: ADDSUBJECT: sex, porn, spam;
- ADDBODY - Adds keywords specified to the body keyword checking database.
  - Example: ADDBODY: free, “100% free”, “absolutely free”;

NOTE

When configuring phrases other than a single words, enclose them in double quotes (“ ”).

Blocklist commands

Use blocklist commands to add a single email address or an entire domain to the email blocklist.

Available commands are:

- `ADDBLIST: <email>;`
  - Example: `ADDBLIST: user@somewhere.com;`

NOTES

1. Add an entire domain to the blocklist by specifying a wildcard before the domain

   Example: `ADDBLIST: *@domain.com;`

2. Wildcards cannot be used in domain names.

   Example: `ADDBLIST: *@*.domain.com;` is invalid and will be rejected.

3. For security reasons, there can be only one `ADDBLIST` command in an email, and only one address can be specified as the command parameter. The parameter is either a user email or a domain:

   Example: `ADDBLIST: spammer@spam.com;` or `ADDBLIST:*@spammers.org;`

Bayesian filter commands

Add spam email or valid email (ham) to the Bayesian filter database. Available commands are:

Command	Description
ADDASSPAM	Instructs Bayesian filter to classify email as spam.
ADDASGOODMAIL	Instructs Bayesian filter to classify email as HAM.

NOTE

These commands do not have parameters - the content of the email is the parameter.

Remote command logging

To keep track of changes made to the configuration database via remote commands, each email with remote commands (even if the email with remote commands was invalid) is saved in:

<GFI MailEssentials installation path>\GFI\MailEssentials\AntiSpam\ADBRProcessed\

The file name of each email is formatted according to the following format:

- `<sender_email_address>_SUCCESS_<timestamp>.eml` - in case of successful processing.
- `<sender_email_address>_FAILED_<timestamp>.eml` - in case of failure.

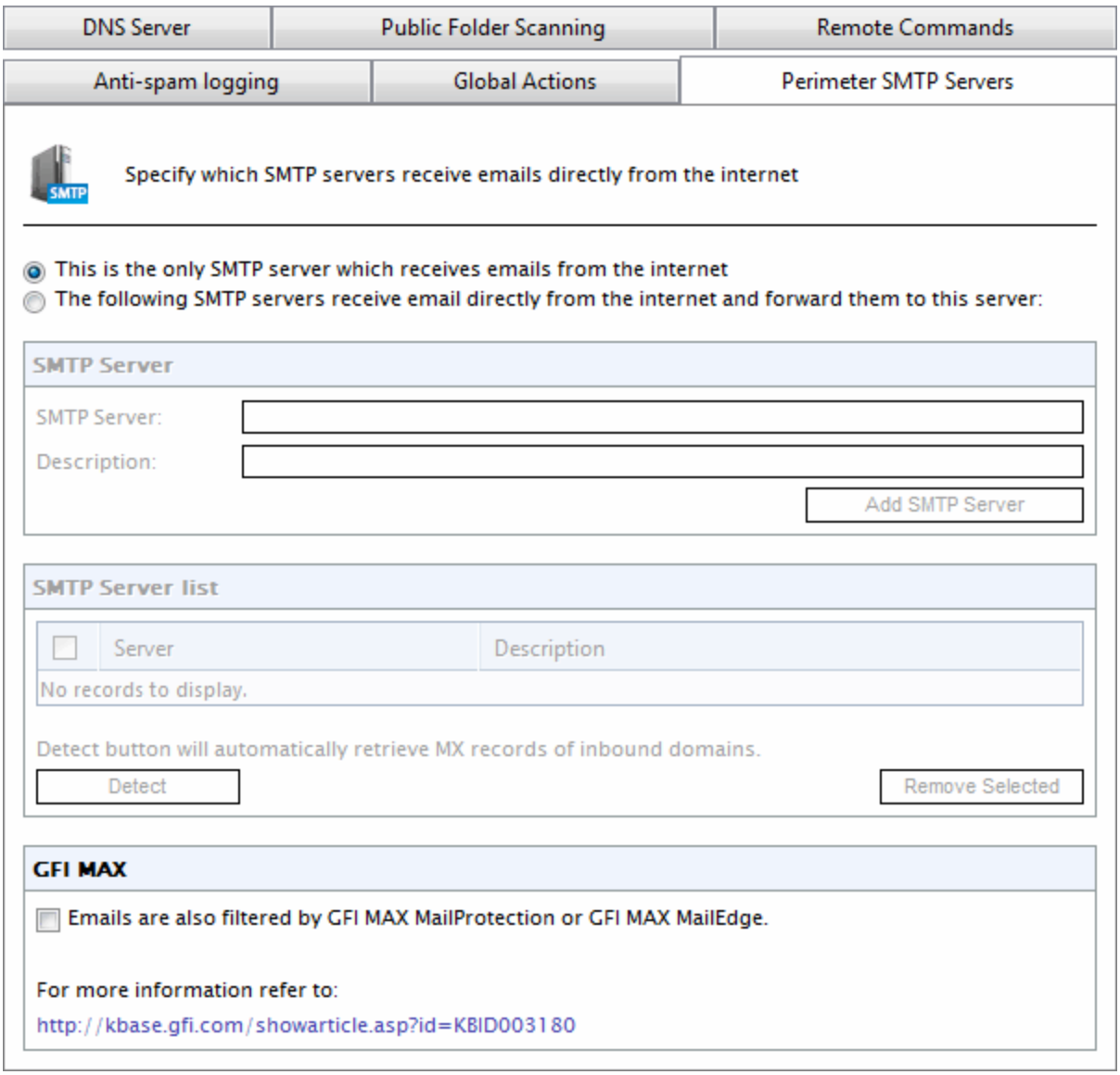
NOTE

Timestamp is formatted as `yyyymmddhhmmss`.

7.5.5 Perimeter SMTP Server Settings

SMTP servers that relay emails to the GFI MailEssentials server must be specified.

1. From the GFI MailEssentials Configuration, go to **Anti-Spam > Anti-Spam Settings**.


DNS Server
Public Folder Scanning
Remote Commands
Anti-spam logging
Global Actions
Perimeter SMTP Servers
SMTP
Specify which SMTP servers receive emails directly from the internet
This is the only SMTP server which receives emails from the internet
The following SMTP servers receive email directly from the internet and forward them to this server:
SMTP Server
SMTP Server:
Description:
Add SMTP Server
SMTP Server list
Server
Description
No records to display.
Detect button will automatically retrieve MX records of inbound domains.
Detect
Remove Selected
GFI MAX
Emails are also filtered by GFI MAX MailProtection or GFI MAX MailEdge.
For more information refer to:
http://kbase.gfi.com/showarticle.asp?id=KBID003180

Screenshot 82: Perimeter SMTP Server settings

2. From the **Perimeter SMTP Servers** tab configure:

Option	Description
This is the only SMTP server which receives emails from the Internet	Select this option when GFI MailEssentials is installed on the only SMTP server that receives external emails directly from the Internet.

Option	Description
The following SMTP servers receive emails directly from the Internet and forward them to this server	Emails are relayed to the GFI MailEssentials server from other SMTP servers. Click **Detect** to instruct GFI MailEssentials to automatically detect SMTP servers by retrieving MX records of inbound domains. Click **Add SMTP Server** to manually add the IPs of any other SMTP servers that relay emails to the GFI MailEssentials server. **NOTE** When manually adding IPs of perimeter SMTP servers, you can also add a range of IP addresses using the CIDR notation.
Emails are also filtered by GFI MAX MailProtection or GFI MAX MailEdge	Select if using hosted email security products GFI MAX MailProtection or GFI MAX MailEdge. For more information refer to: http://go.gfi.com/?pageid=ME_MAXMPME

3. Click **Apply**.

7.6 Public Folder Scanning

Spamming techniques are continuously evolving and consequently you might encounter instances when spam still makes it through anti-spam filters to the recipient's Inbox. Through public folder scanning, users can manually classify email as spam and 'teach' GFI MailEssentials spam patterns to classify similar email as spam. Emails can also be added to the whitelist.

How it works :

1. When an incorrectly classified email (false positive or false negative) is identified, users drag and drop the email to the appropriate GFI AntiSpam public folder. For more information, refer to Using Public folder scanning (page 153).

2. Public folder scanning retrieves emails from the GFI AntiSpam public folders and add to whitelist/blocklist and HAM/SPAM databases.

The GFI Antispam public folders must be created and configured on the mail server. For more information, refer to Enabling Public Folder Scanning (page 149).

Topics in this section:

7.6.1 Enabling Public Folder Scanning 149

7.6.2 Using Public folder scanning 153

7.6.1 Enabling Public Folder Scanning

To enable public folders scanning follow the instructions listed in the sections below:

- Public folder scanning setup for Microsoft ® Exchange Servers
- Configure a dedicated user account for Microsoft ® Exchange Server 2003
- Configure a dedicated user account for Microsoft ® Exchange Server 2007/2010
- Hiding user posts in GFI AntiSpam Folders

NOTE

You can also use GFI MailEssentials with Lotus Domino. For more information refer to Appendix 2 in this guide.

Public folder scanning setup for Microsoft® Exchange Servers

1. From the GFI MailEssentials configuration console go to **Anti-spam** > **Anti-Spam Settings**. Select **Public Folder Scanning** tab.
2. Select **Enable Public Folder Scanning** and from **Poll public folder via** list select:

- **Exchange Server 2003** - Select MAPI, IMAP or WebDAV.
- **Exchange Server 2007** - Choose WebDAV or Web Services.
- **Exchange Server 2010** - Choose Web Services.

Options are described in the table below.

Option	Description
MAPI	To use MAPI, GFI MailEssentials must be installed on the machine on which Microsoft® Exchange Server is installed. No other settings are required.
IMAP	Requires Microsoft® Exchange IMAP service. IMAP enables remote scanning of public folders and works well in environments running firewalls. In addition, IMAP can be used with other Mail servers that support IMAP. Parameters required are: » Mail server name » Port number (default IMAP port is 143) » Username/password » Select the **Use SSL** option to use a secure connection
WebDAV	Specify mail server name, port (default WebDAV port is 80), username/password and domain. To use a secure connection select the **Use SSL** checkbox. By default, public folders are accessible under the 'public' virtual directory. If this has been changed, specify the correct virtual directory name to access the public folders by editing the text in the **URL** box.

Option	Description
Web Services	Specify the following details: » **Server** - mail server name » **Domain** - use the local domain **NOTE** If both a local and a public domain exist, always use the local domain. » **Port** - default Web Services port (80, or 443 if using SSL). » **Username/password** - use credentials with administrative privileges or create a dedicated user from Microsoft ® Exchange® Management Shell by entering the following command to add the appropriate permissions: `Add-ADPermission -identity "Mailbox Store" -User NewUser -AccessRights GenericALL` Replace `Mailbox Store` with the name of the mailbox store that contains the user mailboxes and `NewUser` with the username of the created user. » **Use SSL** - Select this option if Exchange Web Services require a secure connection. By default, Web Services requires SSL. » **URL** - By default, public folders are accessible under the 'EWS/exchange.asmx' virtual directory. If this has been changed, specify the correct virtual directory name to access the public folders by editing the text in the URL box. **NOTE** It is recommended to test the settings manually, by loading the URL in a web browser. This should load an XML formatted file, named **services.wsdl**.

3. Click **Scan Now** to automatically create the Public folders.
4. Click **Test** if you are setting up IMAP, WebDAV or Web Services. On screen notification will confirm success/failure. If the test fails, verify/update credentials and re-test.
5. Click **Apply**.

Configure a dedicated user account for Microsoft ® Exchange Server 2003

For security reasons, it is recommended that when GFI MailEssentials is installed in a DMZ, a dedicated user account is created to retrieve/scan emails from public folders.

1. Create a new Active Directory (AD) user.
2. From the Microsoft® Exchange System Manager, expand **Folders > Public Folders** node.
3. Right click **GFI AntiSpam Folders** public folder and select **Properties**.
4. Click **Permissions** tab and select **Client permissions**.
5. Click **Add…**, select new user, and click **OK**.
6. Select the new user from the client permissions list and from the provided list set its role to **Owner**. Ensure that all checkboxes are selected and the radio buttons are set to **All**.
7. Click **OK** to finalize your configuration.
8. From the Microsoft® Exchange System Manager right click **GFI AntiSpam Folders** and select **All tasks > Propagate settings**.

NOTE

For Microsoft® Exchange Server 2003 SP2, right click **GFI AntiSpam Folders** and select **All tasks > Manage Settings** option.

9. Select **Folder rights or Modify client permissions** and click **OK** or **Next**.
10. Specify the credentials of the new power user account created in step 1 and test the setup to ensure permissions are correct.

Configure a dedicated user account for Microsoft ® Exchange Server 2007/2010

When configuring a dedicated user account to retrieve the emails from the GFI AntiSpam Public folders, the user would need to have 'owner' access rights on the GFI AntiSpam Public Folders.

1. Create a new Active Directory (AD) (power) user.
2. Logon to the Microsoft® Exchange Server using administrative privileges.
3. Open **Microsoft® Exchange Management Shell** and key in following command:

```
Get-PublicFolder -Identity "\GFI AntiSpam Folders" -Recurse | ForEach-
Object {Add-PublicFolderClientPermission -Identity $_.Identity -User
"USERNAME" -AccessRights owner -Server "SERVERNAME"}
```

Change `USERNAME` and `SERVERNAME` to the relevant details of the Active Directory user in question.

Example:

```
Get-PublicFolder -Identity "\GFI AntiSpam Folders" -Recurse | ForEach-
Object {Add-PublicFolderClientPermission -Identity $_.Identity -User
"mesuser" -AccessRights owner -Server "exch07"}
```

Hiding user posts in GFI AntiSpam Folders

For privacy and security purposes, it is highly recommended that you hide user posts made on GFI AntiSpam folders. This way, users will only be able to post to the folders without viewing existing posts (not even the ones they posted themselves). To configure user privileges and hide posts for unauthorized users:

Microsoft ® Exchange 2003

1. From the Microsoft® Exchange System Manager expand **Folders > Public Folders** node.
2. Right click **GFI AntiSpam Folders** public folder and select **Properties**.
3. Select the **Permissions** tab and click **Client permissions**.
4. Click **Add…**, and select the user/group to hide the posts from and click **OK**.
5. Select user/group configured earlier to the client permissions list and set its role to **Contributor**.
6. Ensure that only **Create items** is selected and the radio buttons are set to **None**.
7. Click **OK** to finalize your configuration.

8. From the Microsoft® Exchange System Manager right click **GFI AntiSpam Folders** and select **All tasks > Propagate settings**.

9. Select **Folder rights** checkbox and click **OK**.

Microsoft ® Exchange 2007

1. From **Microsoft ® Exchange Management Shell**, key in the following command:

```
ReplaceUserPermissionOnPFRecursive.ps1 -Server "server" -
TopPublicFolder "\'GFI AntiSpam Folders'" -User "Default" -Permissions
Contributor
```

Replace "`server`" with the full computer name.

2. When prompted, key in `y` to confirm permissions for each folder.

This command will set the default permissions for the GFI MailEssentials Public Folders to contributor, where users can move emails to the Public Folders but cannot view or modify entries. By default administrators are owners of the Public Folders and can view or modify entries. For more information about Public Folders permissions refer to:

http://go.gfi.com/?pageid=ME_PFPermissionsExch2007

Microsoft ® Exchange 2010

1. From Microsoft ® Exchange Management Shell, change the folder to the Microsoft® Exchange scripts folder that can be found in the Microsoft® Exchange installation folder. If Microsoft® Exchange is installed in the default path, the scripts folder is stored in:

```
C:\Program Files\Microsoft\Exchange Server\V14\Scripts\
```

2. Key in the following command:

```
ReplaceUserPermissionOnPFRecursive.ps1 -Server "server" -
TopPublicFolder "\GFI AntiSpam Folders" -User "Default" -Permissions
Contributor
```

Replace "`server`" with the full computer name.

This command will set the default permissions for the GFI MailEssentials Public Folders to contributor, where users can move emails to the Public Folders but cannot view or modify entries. By default administrators are owners of the Public Folders and can view or modify entries. For more information about Public Folders permissions refer to:

http://go.gfi.com/?pageid=ME_PFPermissionsExch2010

7.6.2 Using Public folder scanning

Reviewing spam email

1. When spam emails are delivered to the user's mailbox (in Inbox, Junk E-mail folder or a custom folder) instruct the individual email users to periodically review spam emails.

2. There may be cases where legitimate emails are incorrectly identified as spam (false positives). For more information, refer to Managing legitimate email (page 154).

3. There may also be cases where spam emails are not detected (false negatives). For more information, refer to Managing spam (page 154).

Managing legitimate email

As with any anti-spam solution, GFI MailEssentials might require some time until the optimal anti-spam filtering conditions are achieved. In cases where this is not yet achieved, there might be instances where legitimate email is identified as spam.

In such cases users should add emails incorrectly identified as spam to **Add to whitelist** and **This is legitimate email** folders to 'teach' GFI MailEssentials that the email in question is not spam.

NOTES

1. In Microsoft® Outlook, dragging and dropping email moves the email to the selected folder. To retain a copy of the email, hold down the CTRL key to copy the email rather than moving it.

2. Detailed information how to create the GFI AntiSpam folders is included in this manual. For more information, refer to Enabling Public Folder Scanning (page 149).

Adding senders to the whitelist

1. In the public folders list of the mail client (example, Microsoft® Outlook), locate the **GFI AntiSpam Folders > Add to whitelist** public folder.

2. Drag and drop emails or newsletters to **Add to whitelist** public folder.

Adding discussion lists to the whitelist

Emails sent to discussions lists have the discussion list's email address as the recipient of the message. To receive emails from specific discussion lists, the list's email address needs to be whitelisted.

1. Using your email client, (example, Microsoft® Outlook), locate the **GFI AntiSpam Folders > I want this Discussion list** public folder.

2. Drag and drop discussion lists to the **I want this Discussion list** public folder.

Use legitimate emails to 'teach' the Bayesian filter

1. In the public folders of the mail client (example, Microsoft® Outlook), locate the **GFI AntiSpam Folders > This is legitimate email** public folder.

2. Drag and drop emails to the **This is legitimate email** folder.

Managing spam

While GFI MailEssentials starts identifying spam emails right out of the box, there may be instances where spam makes it through undetected to the users mailbox. Typically this might be either due to configuration settings that have not yet been performed or to new forms of email spam to which GFI MailEssentials has not yet adapted itself. In both cases, these situations are resolved when GFI MailEssentials is configured to capture such spam.

In these cases users should add such emails to **Add to blocklist** and **This is spam email** folders to 'teach' GFI MailEssentials that the email in question is spam.

NOTES

1. In Microsoft® Outlook, dragging and dropping email moves the email to the selected folder. To retain a copy of the email, hold down the CTRL key to copy the email rather than moving it.

2. Detailed information how to create the GFI AntiSpam folders is included in this manual. For more information, refer to Enabling Public Folder Scanning (page 149).

Adding senders to the Email Blocklist

1. In the public folders of the mail client (example, Microsoft® Outlook), locate the **GFI AntiSpam Folders > Add to blocklist** public folder.

2. Drag and drop emails to the **Add to blocklist** public folder.

Use spam emails to 'teach' the Bayesian filter

1. In the public folders of the mail client (example, Microsoft® Outlook), locate the **GFI AntiSpam Folders > This is spam email** public folder.

2. Drag and drop the spam email to the **This is spam email** folder.

8 Content Filtering

Content Filtering engines enable administrators to control the content of emails. These engines scan the content of emails and attachments, and block emails containing content matching the content filtering rules.

Topics in this chapter:

8.1 Keyword Filtering 156
8.1.1 Creating a Keyword Filtering rule 157
8.1.2 Enabling/disabling Rules 162
8.1.3 Removing content filtering rules 162
8.1.4 Modifying an existing rule 162
8.1.5 Changing rule priority 162
8.2 Attachment Filtering 163
8.2.1 Creating an Attachment Filtering rule 163
8.2.2 Enabling/disabling rules 168
8.2.3 Removing attachment rules 169
8.2.4 Modifying an existing rule 169
8.2.5 Changing the rule priority 169
8.3 Advanced Content Filtering 169
8.3.1 Creating Advanced Content Filtering rules 169
8.3.2 Removing Rules 173
8.3.3 Enabling/Disabling Rules 173
8.3.4 Sorting Rules 174
8.4 Decompression Engine 174
8.4.1 Configuring the decompression engine filters 174
8.4.2 Enable/disable decompression filters 179

8.1 Keyword Filtering

Keyword Filtering enables you to set up rules that filter emails with particular keywords or a combination of keywords in the body or subject of the email. A rule is composed of:

- Keywords to block in the email body, subject or attachment
- Actions to take when a keyword is found
- The users to which a rule applies.

To configure content rules, navigate to **Content Filtering > Keyword Filtering**. This page allows you to view, create, enable, disable or delete rules.

8.1.1 Creating a Keyword Filtering rule 157
8.1.2 Enabling/disabling Rules 162
8.1.3 Removing content filtering rules 162
8.1.4 Modifying an existing rule 162

8.1.5 Changing rule priority 162

8.1.1 Creating a Keyword Filtering rule

To create a Keyword filtering rule follow the steps listed below:

- Step 1: Configuring basic rule setting
- Step 2: Configuring terms to block
- Step 3: Configuring the actions to take on detected emails
- Step 4: Specifying the users to whom to apply this rule

Step 1: Configuring basic rule settings

1. Go to **Content Filtering > Keyword Filtering** and select **Add Rule...**
2. Specify a name for the rule in the **Rule name** text box.
3. Select whether to scan inbound, outbound and/or internal emails.

Option	Description
Check Inbound emails	Select this option to scan incoming emails
Check Outbound emails	Select this option to scan outgoing emails
Check Internal emails	Select this option to scan internal emails. **NOTE** This option is only available when GFI MailEssentials is installed on the Microsoft® Exchange server

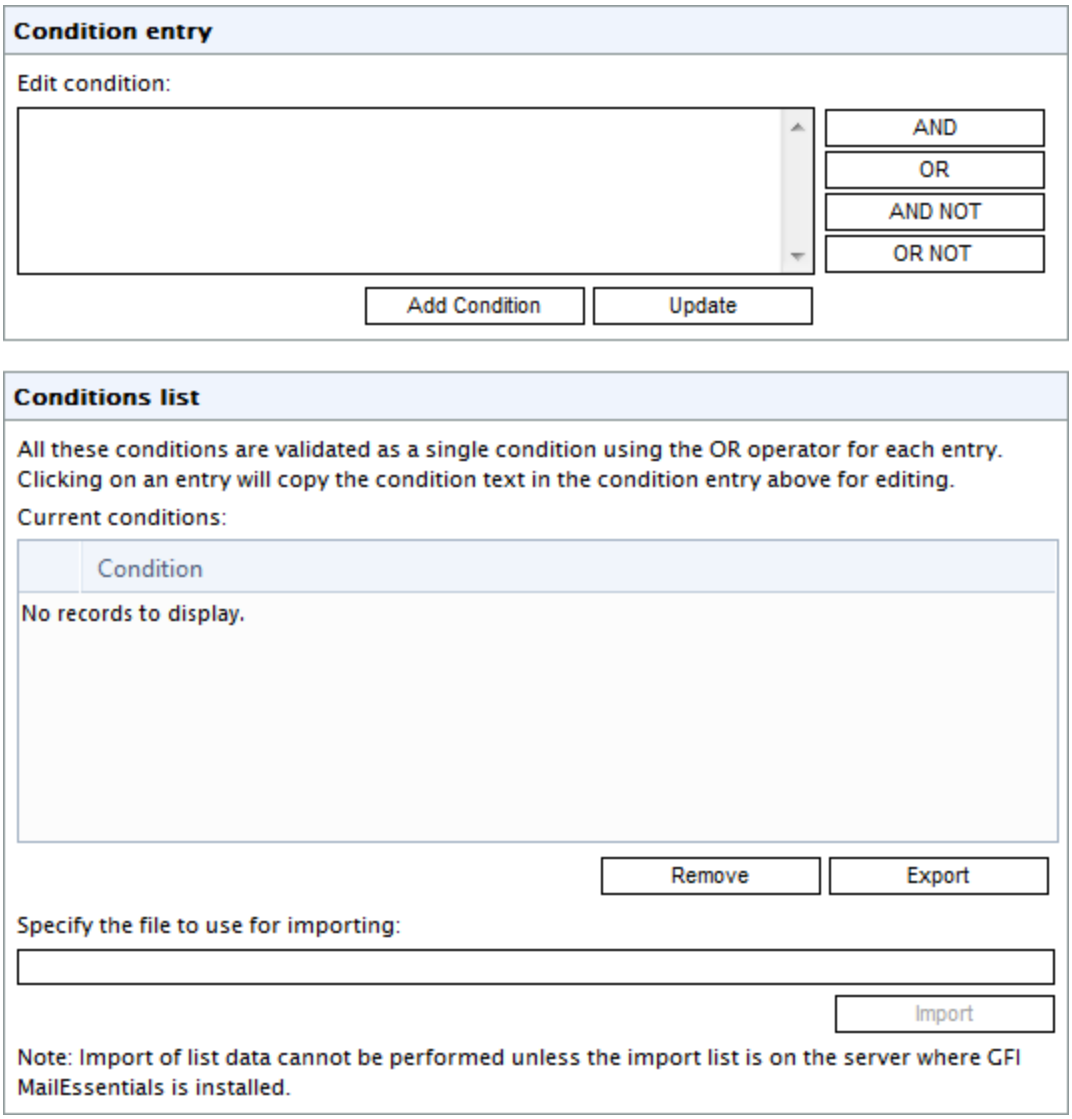
4. To block emails encrypted using PGP technology, select **Block PGP encrypted emails.**

NOTE

PGP encryption is a public-key cryptosystem often used to encrypt emails.

Step 2: Configuring terms to block

1. Select the **Body** tab to specify the keywords in the email body to block.
2. Select **Block emails if content is found matching these conditions (message body/attachments)** checkbox to enable scanning of body for keywords.

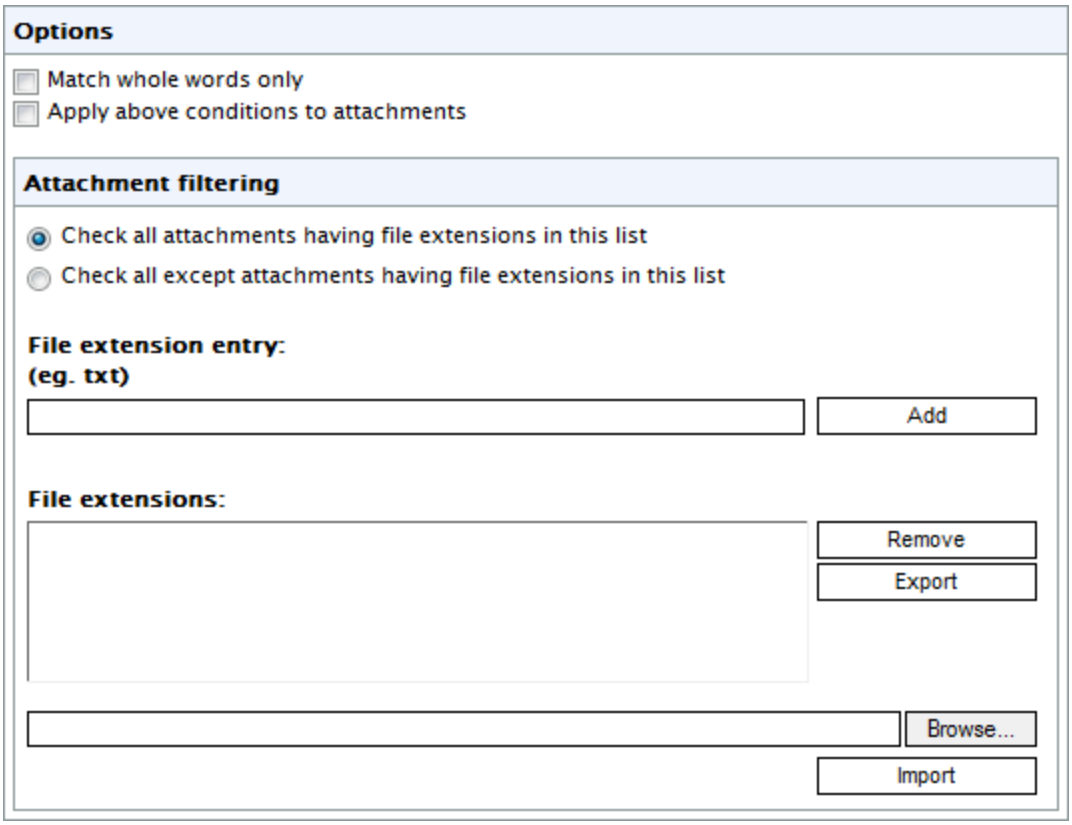

Condition entry
Edit condition:
AND
OR
AND NOT
OR NOT
Add Condition
Update
Conditions list
All these conditions are validated as a single condition using the OR operator for each entry.
Clicking on an entry will copy the condition text in the condition entry above for editing.
Current conditions:
Condition
No records to display.
Remove
Export
Specify the file to use for importing:
Import
Note: Import of list data cannot be performed unless the import list is on the server where GFI MailEssentials is installed.

Screenshot 83: Content Filtering: Body Tab - setting conditions

3. From the **Condition entry** area, key in keywords to block in the **Edit condition** box. You can also use conditions **AND**, **OR**, **AND NOT** and **OR NOT** to use a combinations of keywords.
4. To add the keyword or combination of keywords keyed in, click **Add Condition**.

To modify an entry in the **Conditions** list, select it and make the required changes in the **Condition entry** box. To remove an entry from the **Conditions** list, select it and click **Remove**.

Click **Update** to apply changes.



Screenshot 84: Content Filtering: Body Tab- configuring other options

5. (Optional) From the **Options** area, configure the following settings:

Option	Description
Match whole words only	Block emails when the keywords specified match whole words.
Apply above conditions to attachments	Select this option to apply this rule also to text in attachments. In the **Attachment filtering** area specify the attachments' file extension (for example, `.doc`) to apply or exclude from this rule.

6. Select the **Subject** tab to specify keywords to block in the email subject.
7. From the **Condition entry** area, key in keywords to block in the **Edit condition** box. You can also use conditions **AND**, **OR**, **AND NOT** and **OR NOT** to use a combinations of keywords.
8. To add the keyword or combination of keywords keyed in, click **Add Condition**.

To modify an entry in the **Conditions** list, select it and make the required changes in the **Condition entry** box. To remove an entry from the **Conditions** list, select it and click **Remove**.

Click **Update** to apply changes.

9. From the **Options** area, configure how keywords are matched. Select **Match whole words only** to block emails where the keywords specified match whole words in the subject

Step 3: Configuring the actions to take on detected emails

1. Click the **Actions** tab to configure what should be done when this rule is triggered.
2. To block an email that matches the rule conditions, select **Block email and perform this action** and select one of the following options:

Option	Description
Quarantine email	Stores blocked emails in the Quarantine Store. You can subsequently review (approve/delete) all the quarantined emails. For more information, refer to Quarantine (page 180).
Delete email	Deletes blocked emails.
Move to folder on disk	Moves the email to a folder on disk. Key in the full folder path where to store blocked emails.

IMPORTANT

Actions always affect the whole email containing the blocked content, even if there is other content (such as attachments) that do not trigger this rule.

NOTE

When GFI MailEssentials is installed on same machine as Microsoft® Exchange 2003, GFI MailEssentials may not be able to block outbound emails, but instead replaces the blocked content with a threat report.

3. Select **Send a sanitized copy of the original email to recipient(s)** to choose whether to send a copy of the blocked email to the recipients but with the malicious content removed.
4. GFI MailEssentials can send email notifications whenever an email triggers this filter. To enable this feature, select any of the following options:

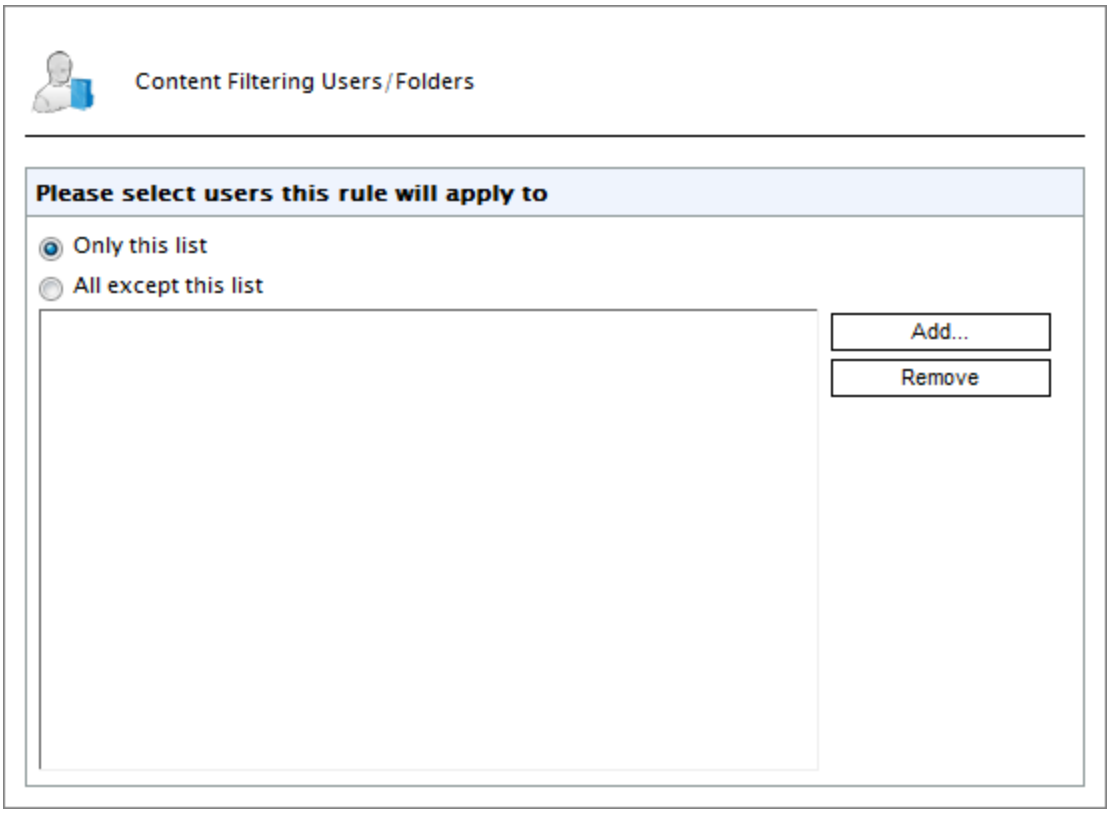
Option	Description
Notify administrator	Notify the administrator whenever this engine blocks an email. For more information, refer to Administrator email address (page 219).
Notify local user	Notify the email local recipients about the blocked email.

5. To log the activity of this engine to a log file select **Log occurrence to this file**. In the text box specify path and file name to a custom location on disk where to store the log file. By default, log files are stored in:

```
<GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\Logs\<EngineName>.log
```

Step 4: Specifying users to whom this rule applies

1. By default, the rule is applied to all email users. GFI MailEssentials, however, allows you to apply this rule to a custom list of email users specified in the Users / Folders tab.

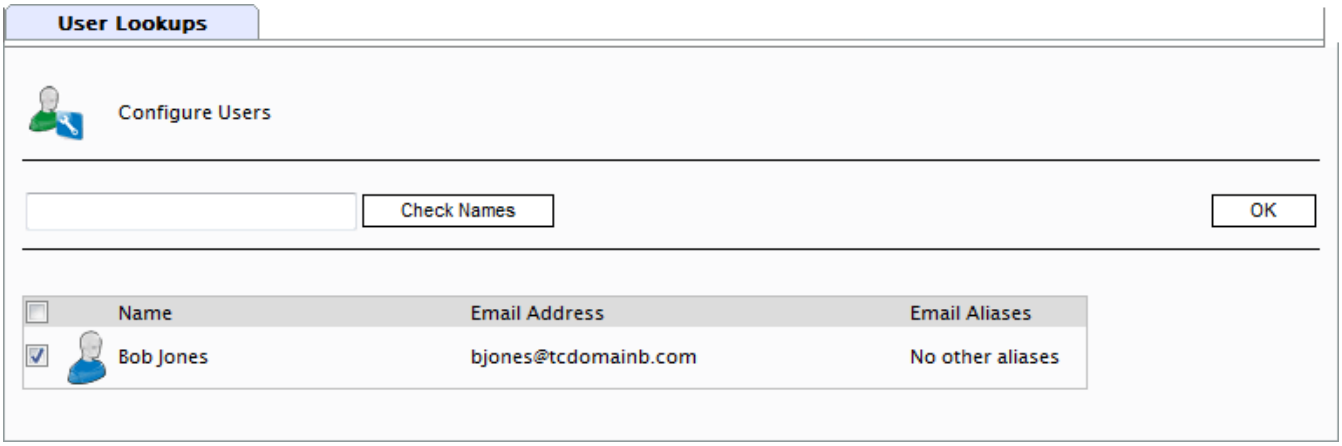


Screenshot 85: Content Filtering: Users/Folders Tab

2. Specify the users to apply this rule to.

Option	Description
Only this list	Apply this rule to a custom list of email users, groups or public folders.
All except this list	Apply this rule to all email users except for the users, groups or public folders specified in the list.

3. To add email users, user groups and/or public folders to the list, click **Add**.



Screenshot 86: Add users to a Content Filtering rule

4. In the **User Lookups** window, specify the name of the email user/user group or public folder that you wish to add to the list and click **Check Names**. Matching users, groups or public folders are listed underneath.

NOTE

You do not need to input the full name of the users, groups or public folder. It is enough to enter part of the name. GFI MailEssentials will list all the names that contain the specified characters. For example, if you input `sco`, GFI MailEssentials will return names such as `Scott Adams` and `Freeman Prescott`, if they are available.

5. Select the check box next to the name(s) that you want to add to the list and click **OK**.

NOTE

To remove entries from the list, select the user/user group/public folder you want to remove and click **Remove**.

6. Repeat steps 3 to 5 to add all the required users to the list.
7. Click **Apply**.

8.1.2 Enabling/disabling Rules

To enable/disable content filtering rules:

1. Go to **Content Filtering > Keyword Filtering**.
2. From the **Content Filtering** page, select the checkbox of the rule(s) to enable or disable.
3. Click **Enable Selected** or **Disable Selected** accordingly

8.1.3 Removing content filtering rules

WARNING

Deleted rules are not recoverable. If in doubt, it is recommended to disable a rule.

1. Go to **Content Filtering > Keyword Filtering**.
2. From the Content Filtering page, select the checkbox of the rule(s) that you want to remove.
3. Click **Remove Selected**.

8.1.4 Modifying an existing rule

1. Go to **Content Filtering > Keyword Filtering**.
2. From the **Content Filtering** page, click the name of the rule to modify.
3. Perform the required changes in the rule properties and click **Apply**.

8.1.5 Changing rule priority

Content Filtering rules are applied in the same order, from top to bottom as they are listed in the Content Filtering page (that is, rule with priority value 1 is checked first). To change the sequence/priority of rules:

1. Go to **Content Filtering > Keyword Filtering**.
2. From the **Content Filtering** page, click the (up) or (down) arrows to respectively increase or decrease the priority of the selected rule.
3. Repeat step 2 until rules are placed in the desired sequence.

8.2 Attachment Filtering

Attachment Filtering allows you to set up rules to filter what types of email attachments to allow and block on the mail server. A rule is composed of:

- Attachment types to block
- Actions to take when a matching attachment is found
- The users to which a rule applies.

To configure attachment rules, navigate to **Content Filtering > Attachment Filtering**. This page allows you to view, create, enable, disable or delete rules.

Topics in this section:

8.2.1 Creating an Attachment Filtering rule 163

8.2.2 Enabling/disabling rules 168

8.2.3 Removing attachment rules 169

8.2.4 Modifying an existing rule 169

8.2.5 Changing the rule priority 169

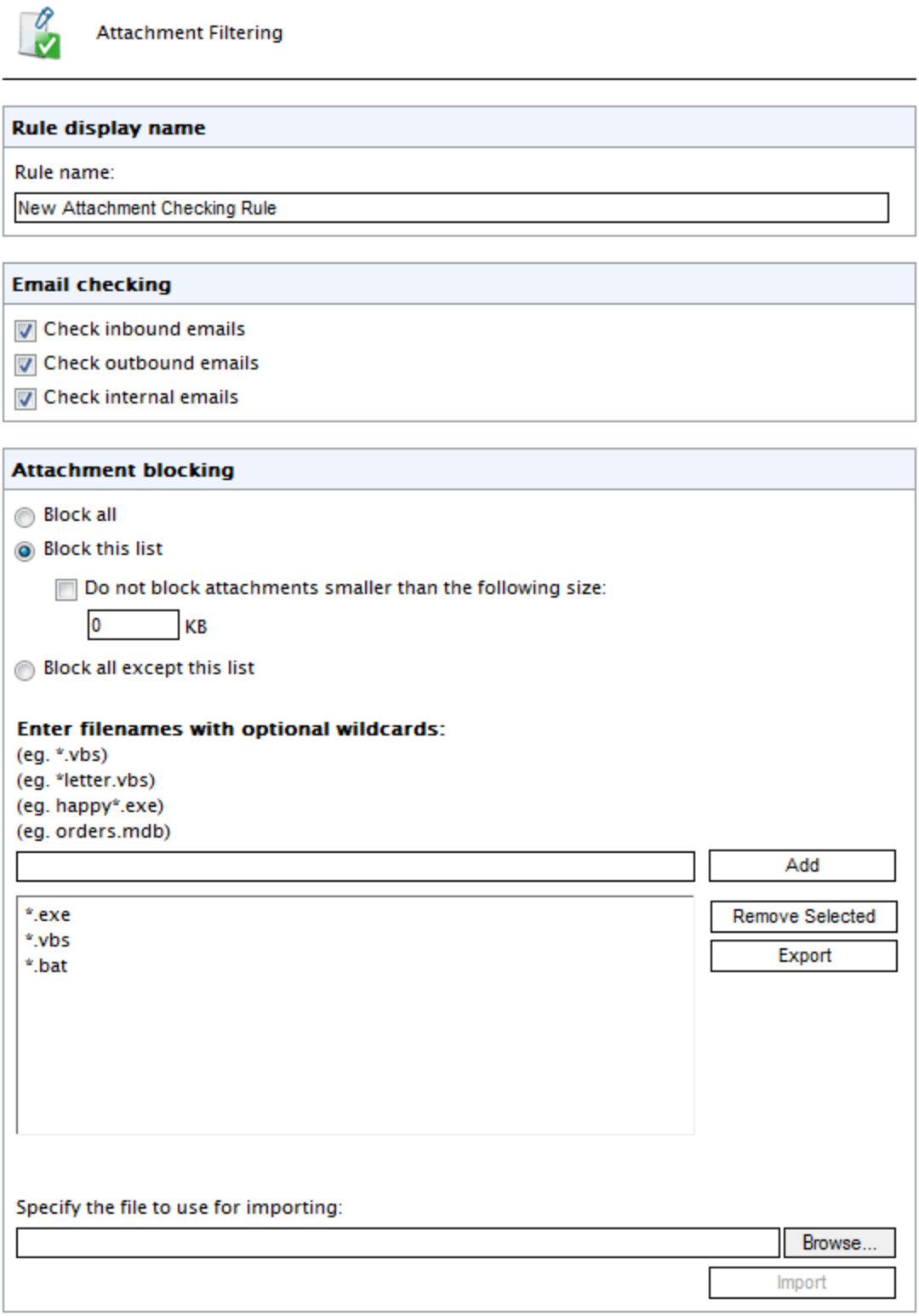
8.2.1 Creating an Attachment Filtering rule

To create an Attachment filtering rule follow the steps listed below:

- Step 1: Configuring basic rule settings and the terms to block
- Step 2: Configuring the actions to take on detected emails
- Step 3: Specifying the users to whom to apply this rule

Step 1: Configuring basic rule settings and the terms to block

1. Navigate to **Content Filtering > Attachment Filtering** node.
2. Click **Add Rule...**



Screenshot 87: Attachment Filtering: General Tab

3. Specify a name for the rule in the **Rule name** text box.
4. Select whether to scan inbound, outbound and/or internal emails.

Option	Description
Check Inbound emails	Select this option to scan incoming emails
Check Outbound emails	Select this option to scan outgoing emails

Option	Description
Check Internal emails	Select this option to scan internal emails. **NOTE** This option is only available when GFI MailEssentials is installed on the Microsoft® Exchange server

5. In the **Attachment Blocking** area, specify the types of attachments to block:

Option	Description
Block all	Block all email attachments of any type.
Block this list	Block a custom list of attachment types. Key in a filename and/or attachment type to block in the **Enter filename with optional wildcards** text box and click **Add**. Repeat this step for all filenames and/or attachment types to block.
Do not block attachments smaller than the following size:	Select this option to allow attachment types in the list that are smaller than a particular size. Specify the size (in KB) in the text box provided.
Block all except this list	Block all attachments except the ones specified in the list. Key in a filename and/or attachment type to allow in the **Enter filename with optional wildcards** text box and click **Add**. Repeat this step for all filenames and/or attachment types to exclude.

NOTE

When specifying filenames and/or attachment types, you can use asterisk (*) wildcards. For example, specifying `*orders*.mdb` refers to all files of type **mdb** that contain the string `orders` in the file name. Specifying `*.jpg` will block all images of type **jpg**.

NOTE

To remove an entry from the list, select it and click **Remove Selected**.

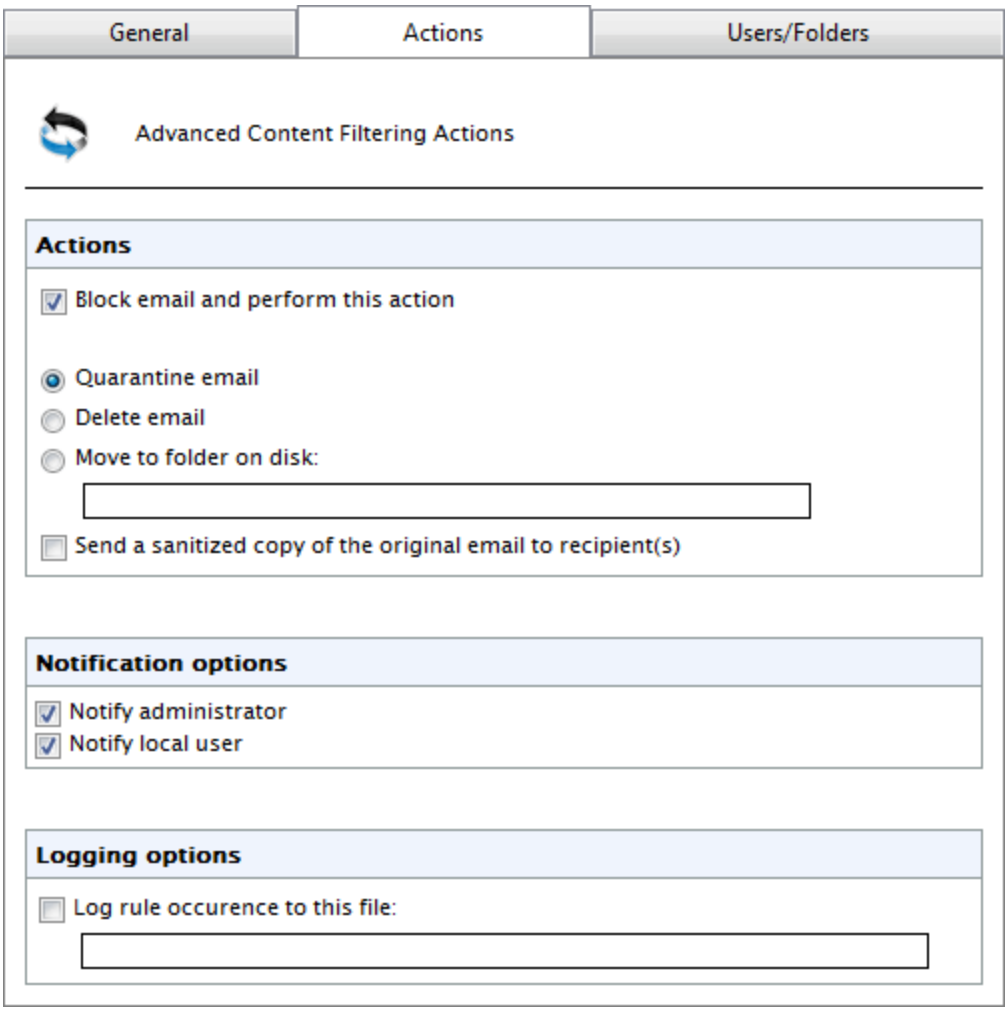
6. You can also block attachments that have a size bigger than a particular size. To enable this option, from the **Options** area select **Block all attachments greater than the following size in KB** and specify the maximum attachment size (in KB).

NOTE

This feature blocks all attachments with a file size bigger than the one specified irrespective if the attachment matches an entry in the **Attachment blocking** list.

Step 2: Configuring the actions to take on detected emails

1. Click the **Actions** tab to configure what happens when this rule is triggered.



Screenshot 88: Attachment Filtering: Actions Tab

2. To block an email that matches the rule conditions, select **Block attachment and perform this action** and select one of the following options:

Option	Description
Quarantine email	Stores blocked emails in the Quarantine Store. You can subsequently review (approve/delete) all the quarantined emails. For more information, refer to Quarantine (page 180).
Delete email	Deletes blocked emails.
Move to folder on disk	Moves the email to a folder on disk. Key in the full folder path where to store blocked emails.

IMPORTANT

Actions always affect the whole email containing the blocked content, even if there is other content (such as attachments) that do not trigger this rule.

NOTE

When GFI MailEssentials is installed on same machine as Microsoft® Exchange 2003, GFI MailEssentials may not be able to block outbound emails, but instead replaces the blocked content with a threat report.

3. Select **Send a sanitized copy of the original email to recipient(s)** to choose whether to send a copy of the blocked email to the recipients but with the malicious content removed.
4. GFI MailEssentials can send email notifications whenever an email triggers this filter. To enable this feature, select any of the following options:

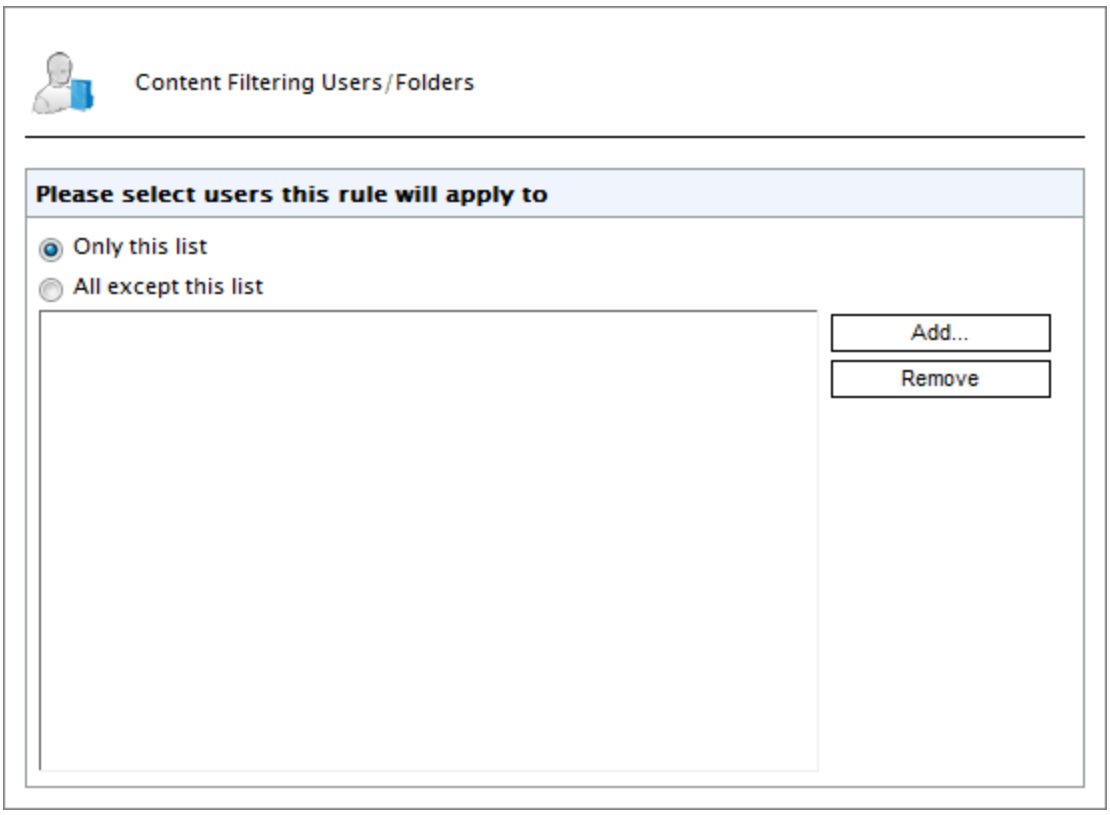
Option	Description
Notify administrator	Notify the administrator whenever this engine blocks an email. For more information, refer to Administrator email address (page 219).
Notify local user	Notify the email local recipients about the blocked email.

5. To log the activity of this engine to a log file select **Log occurrence to this file**. In the text box specify path and file name to a custom location on disk where to store the log file. By default, log files are stored in:

```
<GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\Logs\<EngineName>.log
```

Step 3: Specifying users to whom this rule applies

1. By default, the rule is applied to all email users. GFI MailEssentials, however, allows you to apply this rule to a custom list of email users specified in the Users / Folders tab.

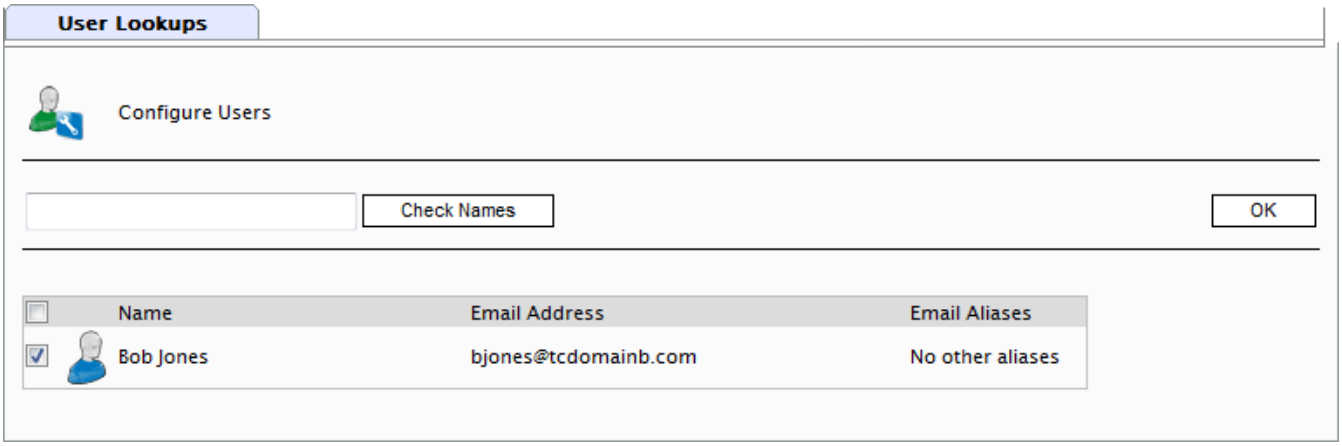


Screenshot 89: Content Filtering: Users/Folders Tab

2. Specify the users to apply this rule to.

Option	Description
Only this list	Apply this rule to a custom list of email users, groups or public folders.
All except this list	Apply this rule to all email users except for the users, groups or public folders specified in the list.

3. To add email users, user groups and/or public folders to the list, click **Add**.



Screenshot 90: Add users to a Content Filtering rule

4. In the **User Lookups** window, specify the name of the email user/user group or public folder that you wish to add to the list and click **Check Names**. Matching users, groups or public folders are listed underneath.

> **NOTE**
>
> You do not need to input the full name of the users, groups or public folder. It is enough to enter part of the name. GFI MailEssentials will list all the names that contain the specified characters. For example, if you input `sco`, GFI MailEssentials will return names such as `Scott Adams` and `Freeman Prescott`, if they are available.

5. Select the check box next to the name(s) that you want to add to the list and click **OK**.

> **NOTE**
>
> To remove entries from the list, select the user/user group/public folder you want to remove and click **Remove**.

6. Repeat steps 3 to 5 to add all the required users to the list.
7. Click **Apply**.

8.2.2 Enabling/disabling rules

To enable or disable attachment filtering rules:

1. Go to **Content Filtering > Attachment Filtering**.
2. From the **Attachment Filtering** page, select the checkbox of the rule(s) to enable or disable.
3. Click **Enable Selected** or **Disable Selected** accordingly.

8.2.3 Removing attachment rules

> **Warning**
>
> Deleted rules are not recoverable. If in doubt, it is recommended to disable a rule.

1. Go to **Content Filtering > Attachment Filtering**.
2. From **Attachment Filtering** page, select the rule(s) that you want to remove.
3. Click **Remove Selected**.

8.2.4 Modifying an existing rule

1. Go to **Content Filtering > Attachment Filtering**.
2. From **Attachment Filtering** page, click the name of the rule to modify.
3. Perform the required changes in the rule properties and click **Apply**.

8.2.5 Changing the rule priority

Attachment Filtering rules are applied in the same order, from top to bottom as they are listed in the Attachment Filtering page (that is, rule with priority value 1 is checked first). To change the sequence/priority of rules:

1. Go to **Content Filtering > Attachment Filtering**.
2. From the Attachment Filtering page, click the (up) or (down) arrows to respectively increase or decrease the priority of the selected rule.
3. Repeat step 2 until rules are placed in the desired sequence.

8.3 Advanced Content Filtering

Advanced Content filtering enables scanning of email header data and content using advanced configurable search conditions and regular expressions (regex).

To configure advanced content rules, go to **Content Filtering > Advanced Content Filtering**. This page allows you to view, create, enable, disable or delete rules.

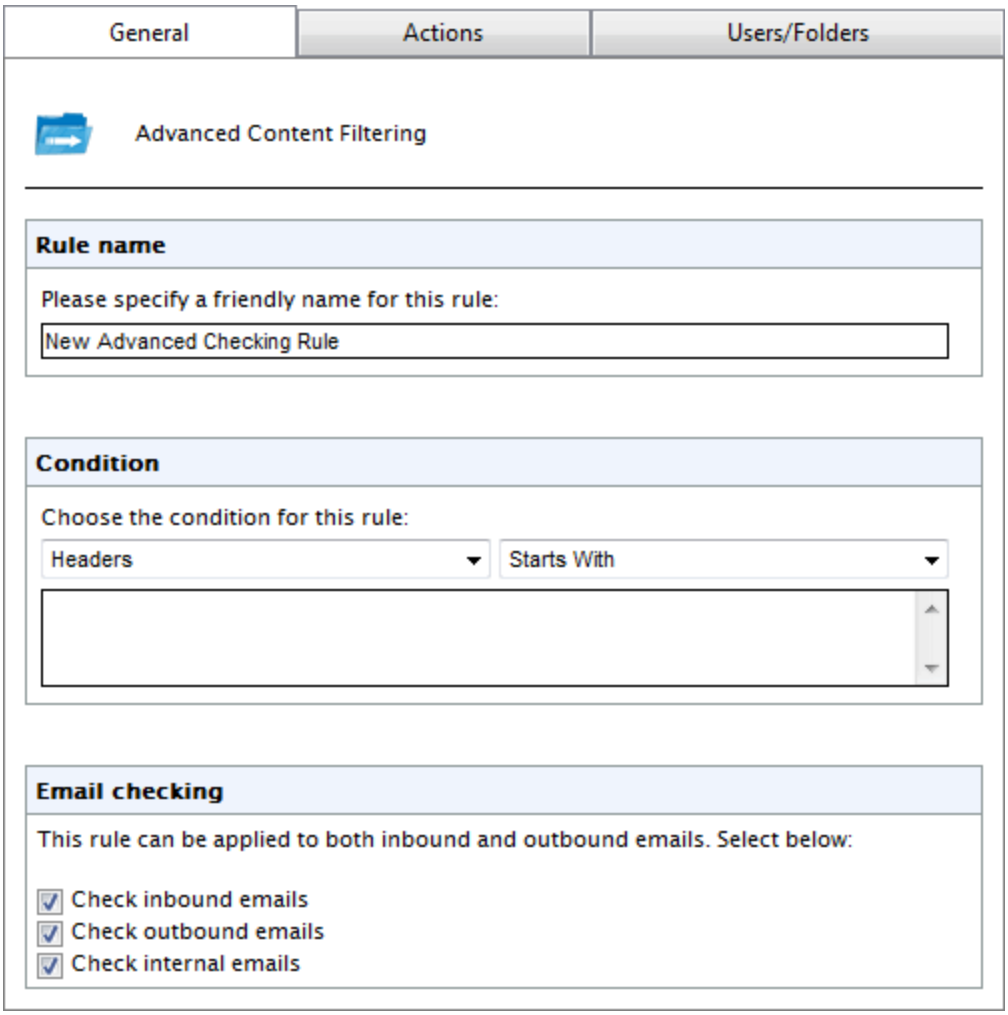
8.3.1 Creating Advanced Content Filtering rules

To create an Advanced Content Filtering rule follow the steps listed below:

- Step 1: Configuring basic rule settings and conditions to block
- Step 2: Configuring the actions to take on detected emails
- Step 3: Specifying the users to whom to apply this rule

Step 1: Configuring basic rule settings and conditions to block

1. Go to **Content Filtering > Advanced Content Filtering** and click **Add Rule...**



Screenshot 91: Adding a new Advanced Content Filtering rule

2. In **Rule Name** area, provide a name for the new rule.

3. In **Condition** area, provide the condition that the email has to meet to match this rule. From the drop down select the email part (**Header**, **Subject**, **Body**, **Attachment Name** or **Attachment Content**) and choose a condition (**Start with**, **Ends with**, **Contains**, **Matches Exactly**, **Matches Regex**). In the text box, key in the keyword or regular expression that the email should match.

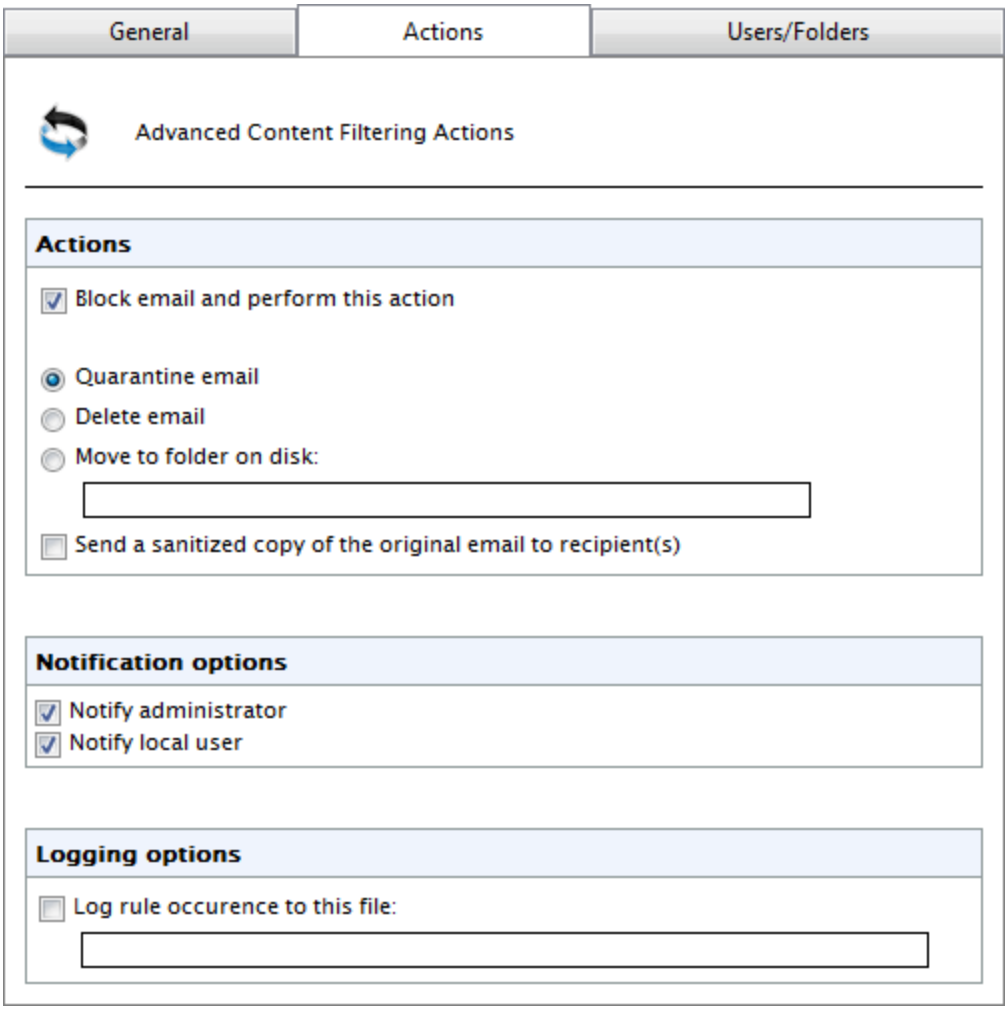
   For example: To match emails having `swiss` in subject - Select **Subject** and **Contains** and key in `swiss` in textbox.

4. Select whether to scan inbound, outbound and/or internal emails.

Option	Description
Check Inbound emails	Select this option to scan incoming emails
Check Outbound emails	Select this option to scan outgoing emails
Check Internal emails	Select this option to scan internal emails. **NOTE** This option is only available when GFI MailEssentials is installed on the Microsoft® Exchange server

Step 2: Configuring the actions to take on detected emails

1. From the **Actions** tab, configure what happens when this rule is triggered.



Screenshot 92: Actions Tab

2. To block an email that matches the rule conditions, select **Block email and perform this action** and select one of the following options:

Option	Description
Quarantine email	Stores blocked emails in the Quarantine Store. You can subsequently review (approve/delete) all the quarantined emails. For more information, refer to Quarantine (page 180).
Delete email	Deletes blocked emails.
Move to folder on disk	Moves the email to a folder on disk. Key in the full folder path where to store blocked emails.

IMPORTANT

Actions always affect the whole email containing the blocked content, even if there is other content (such as attachments) that do not trigger this rule.

NOTE

When GFI MailEssentials is installed on same machine as Microsoft® Exchange 2003, GFI MailEssentials may not be able to block outbound emails, but instead replaces the blocked content with a threat report.

3. Select **Send a sanitized copy of the original email to recipient(s)** to choose whether to send a copy of the blocked email to the recipients but with the malicious content removed.
4. GFI MailEssentials can send email notifications whenever an email triggers this filter. To enable this feature, select any of the following options:

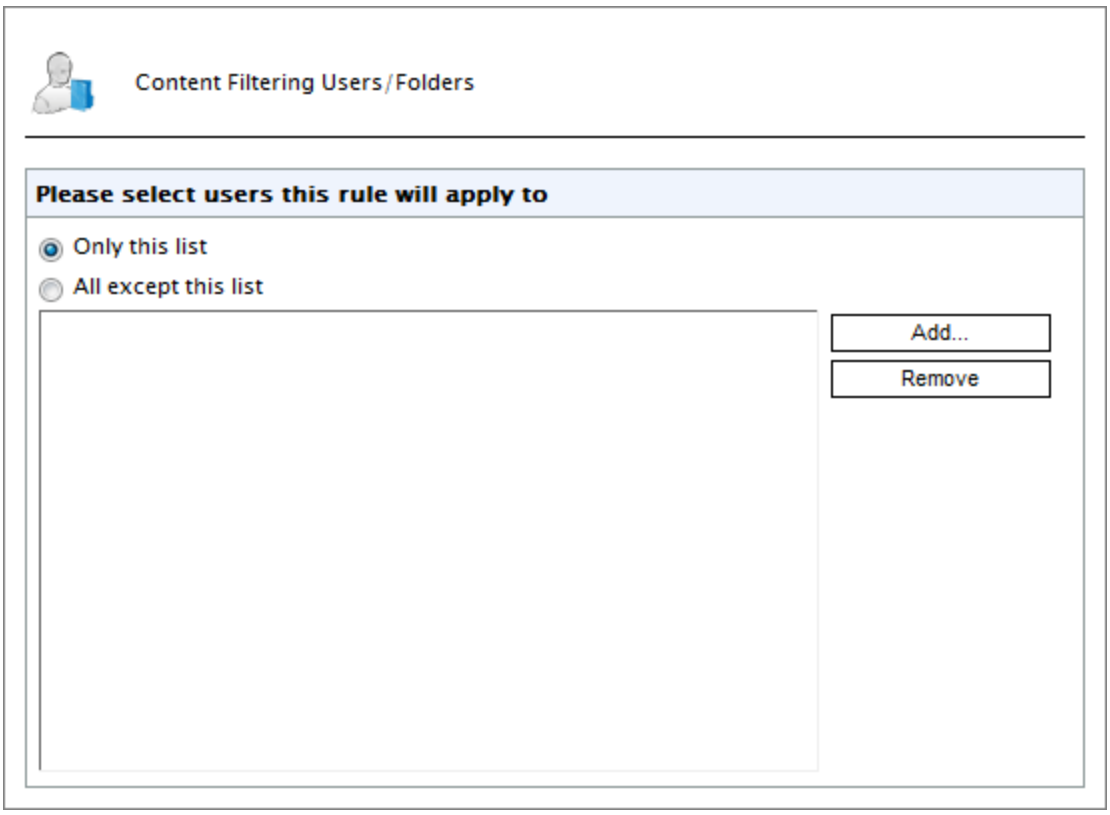
Option	Description
Notify administrator	Notify the administrator whenever this engine blocks an email. For more information, refer to Administrator email address (page 219).
Notify local user	Notify the email local recipients about the blocked email.

5. To log the activity of this engine to a log file select **Log occurrence to this file**. In the text box specify path and file name to a custom location on disk where to store the log file. By default, log files are stored in:

```
<GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\Logs\<EngineName>.log
```

Step 3: Specifying users to whom this rule applies

1. By default, the rule is applied to all email users. GFI MailEssentials, however, allows you to apply this rule to a custom list of email users specified in the Users / Folders tab.

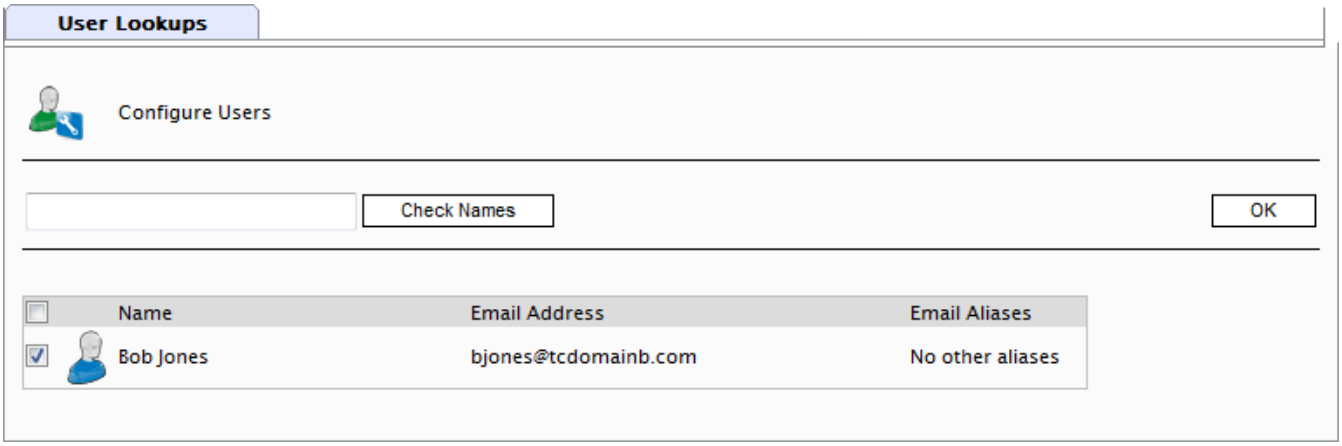


Screenshot 93: Content Filtering: Users/Folders Tab

2. Specify the users to apply this rule to.

Option	Description
Only this list	Apply this rule to a custom list of email users, groups or public folders.
All except this list	Apply this rule to all email users except for the users, groups or public folders specified in the list.

3. To add email users, user groups and/or public folders to the list, click **Add**.



Screenshot 94: Add users to a Content Filtering rule

4. In the **User Lookups** window, specify the name of the email user/user group or public folder that you wish to add to the list and click **Check Names**. Matching users, groups or public folders are listed underneath.

> **NOTE**
>
> You do not need to input the full name of the users, groups or public folder. It is enough to enter part of the name. GFI MailEssentials will list all the names that contain the specified characters. For example, if you input `sco`, GFI MailEssentials will return names such as `Scott Adams` and `Freeman Prescott`, if they are available.

5. Select the check box next to the name(s) that you want to add to the list and click **OK**.

> **NOTE**
>
> To remove entries from the list, select the user/user group/public folder you want to remove and click **Remove**.

6. Repeat steps 3 to 5 to add all the required users to the list.
7. Click **Apply**.

8.3.2 Removing Rules

1. From **Content Filtering > Advanced Content Filtering**, select rule to remove.
2. Click **Remove Selected**.

8.3.3 Enabling/Disabling Rules

1. From **Content Filtering > Advanced Content Filtering**, select rule to enable/disable.
2. Click **Disable Selected** to disable rule or **Enable Selected** to enable.

8.3.4 Sorting Rules

Advanced Content Filtering rules are applied in the same order, from top to bottom as they are listed in the Advanced Content Filtering page (that is, rule with priority value 1 is checked first). To change the sequence/priority of rules:

1. Navigate to the **Content Filtering > Advanced Content Filtering** node.
2. Click the (up) or (down) arrows to respectively increase or decrease the priority of the rule.
3. Repeat step 2 until rules are placed in the desired sequence.

8.4 Decompression Engine

The Decompression engine extracts and analyzes archives (compressed files) attached to an email.

The following is a list of checks performed by the decompression engine:

- Password protected archives
- Corrupted archives
- Recursive archives
- Size of decompressed files in archives
- Amount of files in archives
- Scan within archives

8.4.1 Configuring the decompression engine filters

To configure decompression engine filters:

1. Navigate to **Content Filtering > Decompression** node.

Screenshot 95: Decompression engine checks

2. Click the decompression filter to configure:

- Check password protected archives
- Check corrupted archives
- Check for recursive archives
- Check size of uncompressed files in archives
- Check for amount of files in archives
- Scan within archives

Check password protected archives

1. Navigate to **Content Filtering > Decompression** node.
2. From the list of available filters, click **Check password protected archives**.
3. To enable this filter, select **Check password protected archives**.
4. Specify what to do when an email contains an archive that triggers this filter:

Option	Description
Quarantine	Quarantines blocked emails
Automatically Delete	Deletes blocked emails

> **NOTE**
>
> When GFI MailEssentials is installed on same machine as Microsoft® Exchange 2003, GFI MailEssentials may not be able to block outbound emails, but instead replaces the blocked content with a threat report.

5. Select **Send a sanitized copy of the original email to recipient(s)** to choose whether to send a copy of the blocked email to the recipients.
6. Click the **Actions** tab to configure further actions.
7. GFI MailEssentials can send email notifications whenever an email triggers this filter. To enable this feature, select any of the following options:

Option	Description
Notify administrator	Notify the administrator whenever this engine blocks an email. For more information, refer to Administrator email address (page 219).
Notify local user	Notify the email local recipients about the blocked email.

8. To log the activity of this engine to a log file select **Log occurrence to this file**. In the text box specify path and file name to a custom location on disk where to store the log file. By default, log files are stored in:

```
<GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\Logs\<EngineName>.log
```

9. Click **Apply**.

Check corrupted archives

1. Navigate to **Content Filtering > Decompression** node.

2. From the list of available filters, click **Check corrupted archives**.
3. To enable this filter select **Check corrupted archives**.
4. Specify what to do when an email contains an archive that triggers this filter:

Option	Description
Quarantine	Quarantines blocked emails
Automatically Delete	Deletes blocked emails

> **NOTE**
>
> When GFI MailEssentials is installed on same machine as Microsoft® Exchange 2003, GFI MailEssentials may not be able to block outbound emails, but instead replaces the blocked content with a threat report.

5. Select **Send a sanitized copy of the original email to recipient(s)** to choose whether to send a copy of the blocked email to the recipients.
6. Click the **Actions** tab to configure further actions.
7. GFI MailEssentials can send email notifications whenever an email triggers this filter. To enable this feature, select any of the following options:

Option	Description
Notify administrator	Notify the administrator whenever this engine blocks an email. For more information, refer to Administrator email address (page 219).
Notify local user	Notify the email local recipients about the blocked email.

8. To log the activity of this engine to a log file select **Log occurrence to this file**. In the text box specify path and file name to a custom location on disk where to store the log file. By default, log files are stored in:

```
<GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\Logs\<EngineName>.log
```

9. Click **Apply**

Check for recursive archives

This filter allows you to quarantine or delete emails that contain recursive archives. Recursive archives, also known as nested archives, are archives that contain multiple levels of sub-archives (that is, archives within archives). A high number of archive levels can indicate a malicious archive. Recursive archives can be used in a DoS (Denial of Service) attack, since recursive archives consume machine resources when they are being analyzed. To configure this filter:

1. Navigate to **Content Filtering > Decompression** node.
2. From the list of available filters, click **Check for recursive archives**.
3. To enable this filter select **Check for recursive archives**.
4. Specify the maximum number of recurring archives in the **Maximum number of recurring archives** text box. If an archive contains more recurring archives than the specified number, the

email is triggered as malicious.

5. Specify what to do when an email contains an archive that triggers this filter:

Option	Description
Quarantine	Quarantines blocked emails
Automatically Delete	Deletes blocked emails

> **NOTE**
>
> When GFI MailEssentials is installed on same machine as Microsoft® Exchange 2003, GFI MailEssentials may not be able to block outbound emails, but instead replaces the blocked content with a threat report.

6. Select **Send a sanitized copy of the original email to recipient(s)** to choose whether to forward a copy of the blocked email to the recipients but with the malicious content removed.
7. Click the **Actions** tab to configure further actions.
8. GFI MailEssentials can send email notifications whenever an email triggers this filter. To enable this feature, select any of the following options:

Option	Description
Notify administrator	Notify the administrator whenever this engine blocks an email. For more information, refer to Administrator email address (page 219).
Notify local user	Notify the email local recipients about the blocked email.

9. To log the activity of this engine to a log file select **Log occurrence to this file**. In the text box specify path and file name to a custom location on disk where to store the log file. By default, log files are stored in:

```
<GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\Logs\<EngineName>.log
```

10. Click **Apply**.

Check size of uncompressed files in archives

This filter allows you to block or delete emails with archives that exceed the specified physical size when uncompressed. Hackers sometimes use this method in a DoS (Denial of Service) attack by sending an archive that can be uncompressed to a very large file that consumes hard disk space and takes a long time to analyze by content security or antivirus software.

To configure this filter:

1. Navigate to **Content Filtering > Decompression** node.
2. From the list of available filters, click **Check size of uncompressed files in archives**.
3. To enable this filter select **Check size of uncompressed files in archives**.
4. Specify the maximum size of uncompressed archives in the Maximum **size of uncompressed files in archive in MB** text box. If an uncompressed archive's size is bigger than the specified value, the email is triggered as malicious.
5. Specify what to do when an email contains an archive that triggers this filter:

Option	Description
Quarantine	Quarantines blocked emails
Automatically Delete	Deletes blocked emails

NOTE

When GFI MailEssentials is installed on same machine as Microsoft® Exchange 2003, GFI MailEssentials may not be able to block outbound emails, but instead replaces the blocked content with a threat report.

6. Select **Send a sanitized copy of the original email to recipient(s)** to choose whether to send a copy of the blocked email to the recipients but with the malicious content removed.
7. GFI MailEssentials can send email notifications whenever an email triggers this filter. To enable this feature, select any of the following options:

Option	Description
Notify administrator	Notify the administrator whenever this engine blocks an email. For more information, refer to Administrator email address (page 219).
Notify local user	Notify the email local recipients about the blocked email.

8. To log the activity of this engine to a log file select **Log occurrence to this file**. In the text box specify path and file name to a custom location on disk where to store the log file. By default, log files are stored in:

```
<GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\Logs\<EngineName>.log
```

9. Click **Apply**.

Check for amount of files in archives

This filter allows you to quarantine or delete emails that contain an excessive amount of compressed files within an attached archive. You can specify the number of files allowed in archive attachments from the configuration options included in this filter. To configure this filter:

1. Navigate to **Content Filtering > Decompression** node.
2. From the list of available filters, click **Check for amount of files in archives**.
3. To enable this filter select **Check for amount of files in archives**.
4. Specify the maximum number of files in archives in the **If the number of files within archive exceeds** text box. If the archive contains more files than the specified value, the email is triggered as malicious.
5. Specify what to do when an email contains an archive that triggers this filter:

Option	Description
Quarantine	Quarantines blocked emails
Automatically Delete	Deletes blocked emails

NOTE

When GFI MailEssentials is installed on same machine as Microsoft® Exchange 2003, GFI MailEssentials may not be able to block outbound emails, but instead replaces the blocked content with a threat report.

6. Select **Send a sanitized copy of the original email to recipient(s)** to choose whether to send a copy of the blocked email to the recipients.
7. Click the **Actions** tab to configure further actions.
8. GFI MailEssentials can send email notifications whenever an email triggers this filter. To enable this feature, select any of the following options:

Option	Description
Notify administrator	Notify the administrator whenever this engine blocks an email. For more information, refer to Administrator email address (page 219).
Notify local user	Notify the email local recipients about the blocked email.

9. To log the activity of this engine to a log file select **Log occurrence to this file**. In the text box specify path and file name to a custom location on disk where to store the log file. By default, log files are stored in:

```
<GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\Logs\<EngineName>.log
```

10. Click **Apply**.

Scan within archives

You can configure GFI MailEssentials to apply Keyword and Attachment Filtering of files within archives.

1. Navigate to **Content Filtering > Decompression** node.
2. From the list of available filters, click **Scan within archives**.
3. To enable scanning within archives select **Apply Attachment and Content Filtering rules within archives**. For more information, refer to Content Filtering (page 156).
4. Click **Apply**.

8.4.2 Enable/disable decompression filters

To enable or disable decompression filters:

1. Navigate to **Content Filtering > Decompression** node.
2. From the **Decompression engine** page, select the checkbox of the filters to enable or disable.
3. Click **Enable Selected** or **Disable Selected** accordingly.

9 Quarantine

The GFI MailEssentials Quarantine feature provides a central store where all emails detected as spam or malware are retained. This ensures that users do not receive spam and malware in their mailbox and processing on the mail server is reduced.

Administrators and mail users can review quarantined emails by accessing the quarantine interface from a web browser. GFI MailEssentials can also send regular email reports to email users to review their blocked emails.

Refer to the following sections for more information on configuring the GFI MailEssentials Quarantine.

9.1 Important Notes 180

9.2 Searching the quarantine 180

9.3 Search Folders 185

9.4 Working with Quarantined emails 187

9.5 Quarantine RSS Feeds 190

9.6 Quarantine Options 192

9.7 Quarantine Store Location and Public URL 198

9.1 Important Notes

1. To quarantine spam or malicious emails, change the filters' and engines' actions to **Quarantine email**.
2. The Quarantine Store requires disk space to retain the organization's spam email or malware for a number of days. The amount of disk space required depends on:
   - The quantity received
   - How long it is retained.
3. On average, 100,000 spam or malware emails of 5 KB each will require approximately 600 MB of disk space to store the email and its metadata.
4. If the free disk space where the Quarantine Store is saved is 512 MB or less, GFI MailEssentials stops quarantining spam and malware; it is instead tagged and delivered to recipients' mailboxes until free disk space increases to more than 512 MB. This ensures that the disk will not run out of space.

9.2 Searching the quarantine

The Quarantine Store is accessible from the GFI MailEssentials interface and allows management of quarantined emails.

To access the GFI MailEssentials Quarantine Store, go to **GFI MailEssentials > Quarantine**.

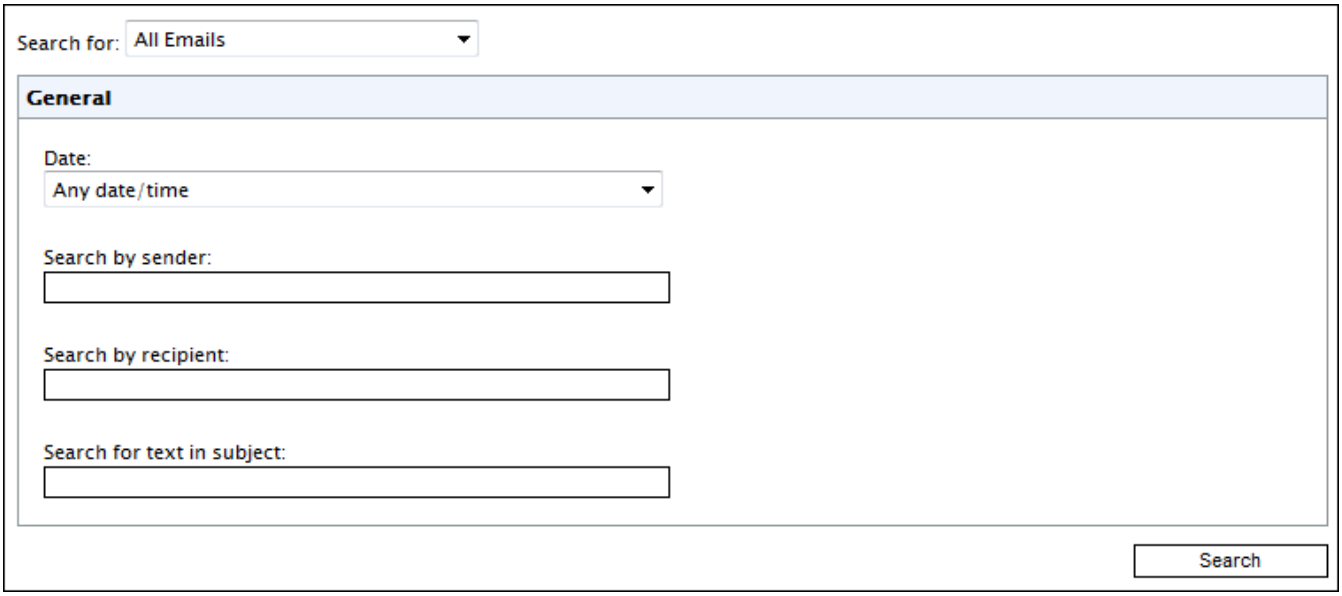
There are various ways how to search for content in the GFI MailEssentials Quarantine:

- Searching though quarantined Malware and Spam
- Searching through Malware emails only

- Search through Spam emails only

Search through both Malware and Spam

1. Go to **GFI MailEssentials > Quarantine**.



Screenshot 96: Malware and Spam Search Area

2. From the **Quarantine** page, select **All Emails** from **Search for** dropdown.
3. Specify the required search criteria.

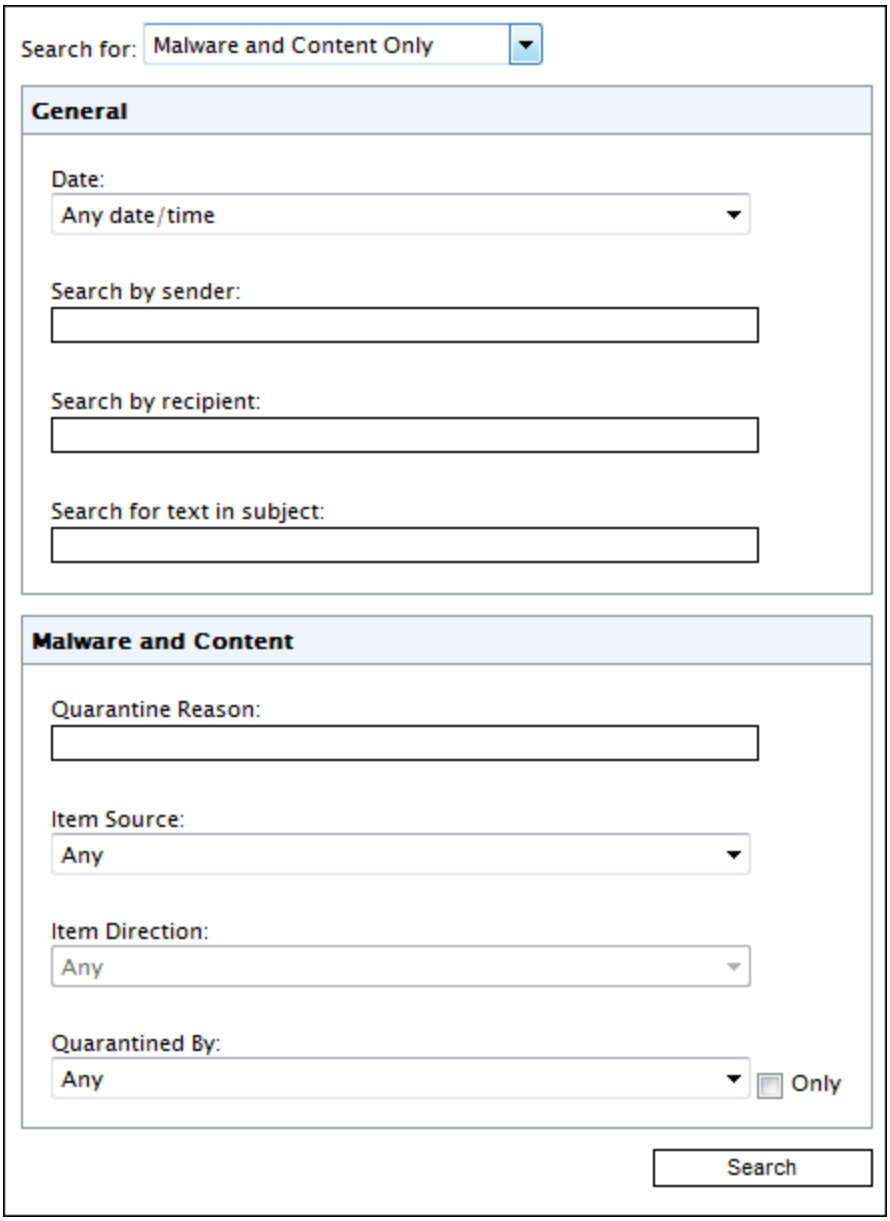
SEARCH CRITERIA	DESCRIPTION
Date:	Select the date range when the email was quarantined. Available date ranges are: » Any date/time » Since yesterday » Last 7 days » Last 30 days » Custom date range
Search by sender	Specify a sender who sent the email that was quarantined.
Search by recipient	Specify a recipient for whom an email was quarantined.
Search for text in subject	Specify the text to search for within quarantined email subject.

4. Click **Search**.

> **NOTE**
>
> Use the search results to review quarantined emails. You can approve false positives for delivery to recipients. For more information, refer to Working with Quarantined emails (page 187).

Search for Malware and Content only

1. Go to **GFI MailEssentials > Quarantine**.



Screenshot 97: Malware and Spam Search Area

2. From the **Quarantine** page, select **Malware and Content Only** from **Search for** dropdown.
3. Specify the required search criteria.

SEARCH CRITERIA	DESCRIPTION
Date:	Select the date range when the email was quarantined. Available date ranges are: » Any date/time » Since yesterday » Last 7 days » Last 30 days » Custom date range
Search by sender	Specify a sender who sent the email that was quarantined.
Search by recipient	Specify a recipient for whom an email was quarantined.

SEARCH CRITERIA	DESCRIPTION
Search for text in subject	Specify the text to search for within quarantined email subject.
Quarantine Reason	Key in the reason for which the email to search for was quarantined.
Item Source	Select the source from where email was identified as Malware and quarantined. Available options are: » Information Store (VSAPI) » Gateway (SMTP) » Information Store (Transport)
Item Direction	Select the direction of the quarantined email to search for, » Any » Inbound » Outbound **NOTE** This option is available only if **Gateway (SMTP)** is selected in **Item Source**.
Quarantined by	Select one of the GFI MailEssentials filters that quarantined the email. Select **Only** checkbox to search for emails quarantined only by a specific filter.

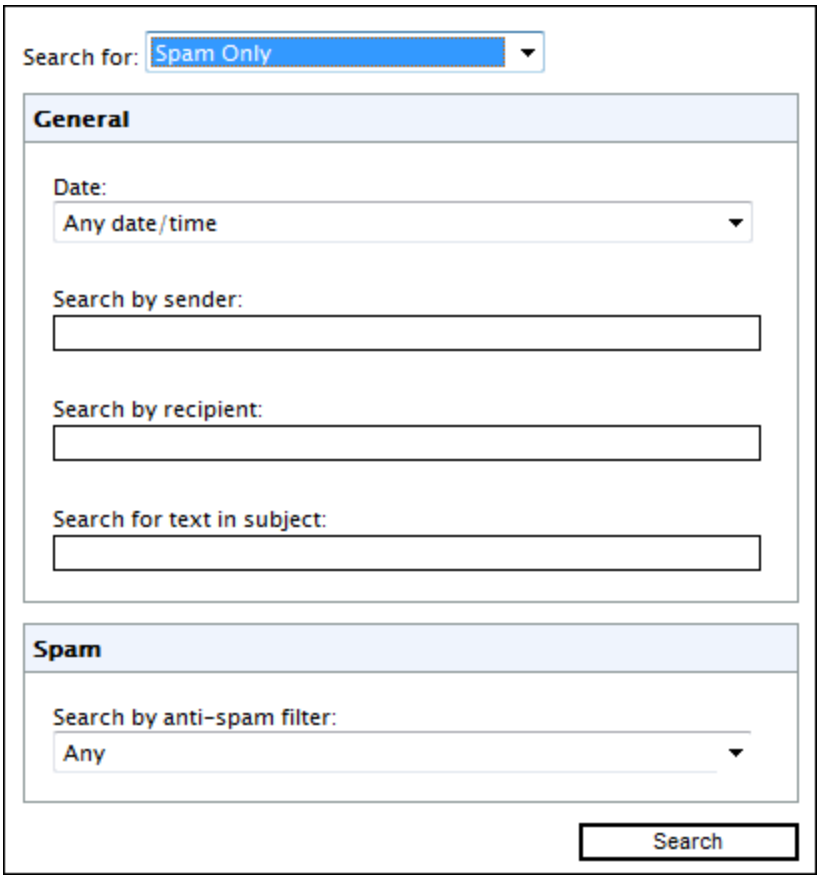
4. Click **Search**.

NOTE

Use the search results to review quarantined emails. You can approve false positives for delivery to recipients. For more information, refer to Working with Quarantined emails (page 187).

Search for Spam Only

1. Go to **GFI MailEssentials > Quarantine**.



Screenshot 98: Spam Only search area

2. From the **Quarantine** page, select **Spam Only** from **Search for** dropdown.
3. Specify the required search criteria. Available options are:

SEARCH CRITERIA	DESCRIPTION
Date:	Select the date range when the email was quarantined. Available date ranges are: » Any date/time » Since yesterday » Last 7 days » Last 30 days » Custom date range
Search by sender	Specify a sender who sent the email that was quarantined.
Search by recipient	Specify a recipient for whom an email was quarantined.
Search for text in subject	Specify the text to search for within quarantined email subject.
Search by anti-spam filter	Select the anti-spam filter that identified the email to search for as Spam.

4. Click **Search**.

NOTE

Use the search results to review quarantined emails. You can approve false positives for delivery to recipients. For more information, refer to Working with Quarantined emails (page 187).

9.3 Search Folders

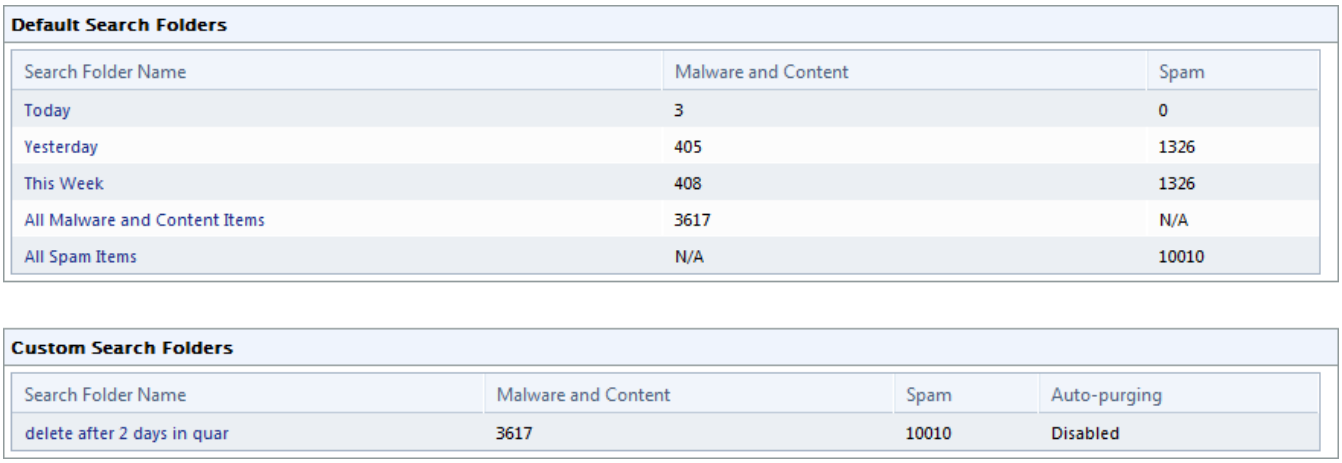
A Search Folder is a folder that has a custom search query associated to it and displays all quarantined emails that match the search query.

Examples of search folders:

- A search folder that displays only outbound emails quarantined by the Virus Scanning Engines.
- A search folder that displays inbound emails quarantined in a particular date range and addressed to a particular user.
- A search folder that displays emails that meet specific search criteria
- A search folder that displays the results of a previously defined search query.

To display emails in a particular search folder:

1. Go to **Quarantine** node.



Default Search Folders

Search Folder Name	Malware and Content	Spam
Today	3	0
Yesterday	405	1326
This Week	408	1326
All Malware and Content Items	3617	N/A
All Spam Items	N/A	10010

Custom Search Folders

Search Folder Name	Malware and Content	Spam	Auto-purging
delete after 2 days in quar	3617	10010	Disabled

Screenshot 99: Default and custom search folders

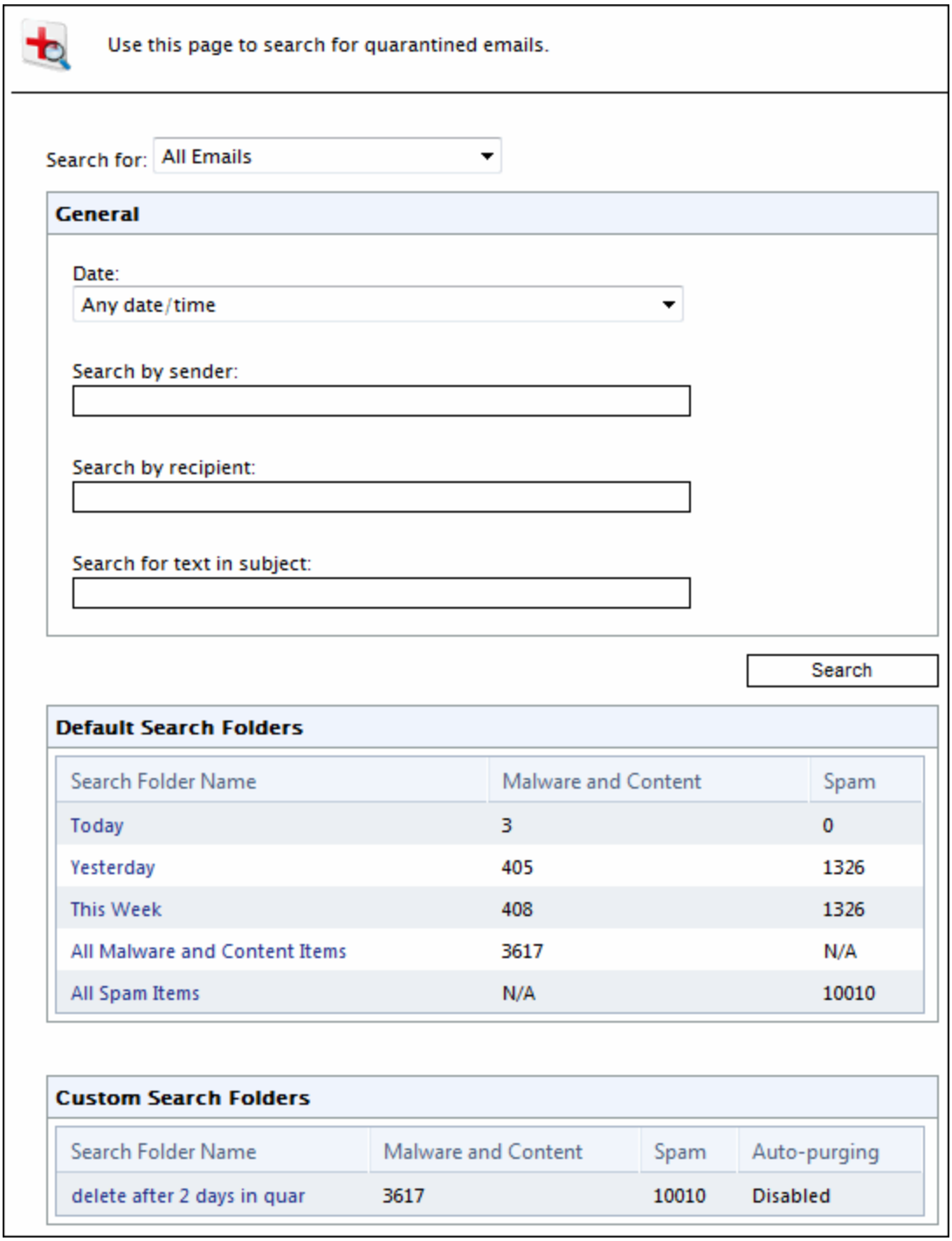
2. Click a search folder displayed in the **Default Search Folders** or **Custom Search Folders** areas. Alternatively, select one of the search folder nodes under the **Quarantine** and **Quarantine > Search Folders** node.

> **NOTE**
>
> Use the search results to review quarantined emails. You can approve false positives for delivery to recipients. For more information, refer to Working with Quarantined emails (page 187).

9.3.1 Default Search Folders

Default Search Folders are preconfigured search folders that enable you to access quarantined emails according to specific time periods or by a specific quarantined email type. To use the default search folders:

1. Go to **Quarantine** node.



Screenshot 100: Default search folders

2. Select a search folder from the **Default Search Folders** area or from a node beneath **Quarantine** node to access the search folder. GFI MailEssentials will automatically search for and display all quarantined emails that satisfy the default search folder search criteria.

Available default search folders are:

» **Time based:**

- Today
- Yesterday
- This week

» **Category based:**

- All Malware and Content Items
- All Spam Items

> **NOTE**
>
> Use the search results to review quarantined emails. You can approve false positives for delivery to recipients. For more information, refer to Working with Quarantined emails (page 187).

9.3.2 Creating, editing and removing Custom Search Folders from Searches

1. Go to **Quarantine** node.
2. Create a new search for quarantined emails. For more information, refer to Searching the quarantine (page 180).
3. In the results page, click **Save as Search Folder** and key in an easily identifiable name for the new Search Folder.

The newly created search folder is listed in **Quarantine > Search Folders** node.

> **NOTE**
>
> To edit or delete a previously created search folder, access the search folder and click **Edit Search Folder** or **Delete Search folder**.

9.3.3 Using the Search Folders node to auto-purge quarantined emails

The **Search Folders** node enables you to create Search folders and set an auto-purge value (in days).When a quarantined email exceeds the specified number of days in the quarantine, the email is deleted.

1. Select **Quarantine > Search Folders** node.
2. Configure a new search folder for the emails to purge on a regular basis using the instructions in this chapter.
3. Select **Enable Auto-purging** and provide the number of days to keep emails for.
4. Click **Save Folder**.

9.4 Working with Quarantined emails

Within GFI MailEssentials there are a number of actions you can take on quarantined emails.

The Quarantine Store is accessible from the GFI MailEssentials interface and the administrator can manage quarantined emails.

To access the GFI MailEssentials Quarantine Store, go to **GFI MailEssentials > Quarantine**.

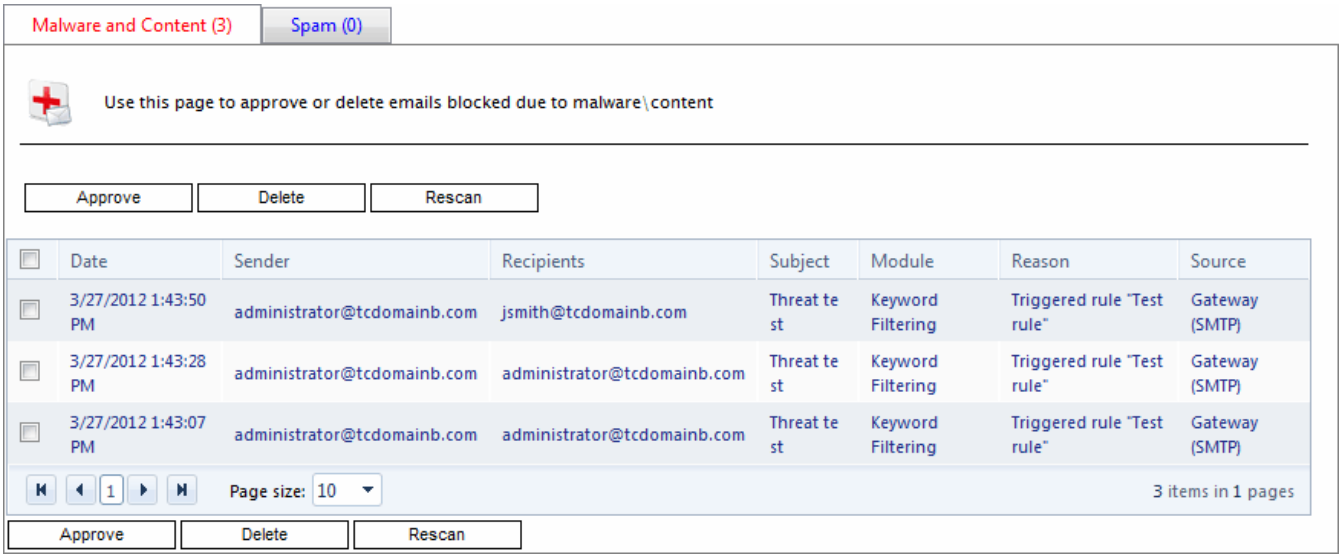
9.4.1 Viewing quarantined emails 188

9.4.2 Approving Quarantined Emails 189

9.4.3 Permanently Delete Quarantined Emails 190

9.4.1 Viewing quarantined emails

Searching within the Quarantine or using default or customized search folders yields a list of quarantined emails.



Screenshot 101: Search Results

NOTE

The results page may be split in two tabs:

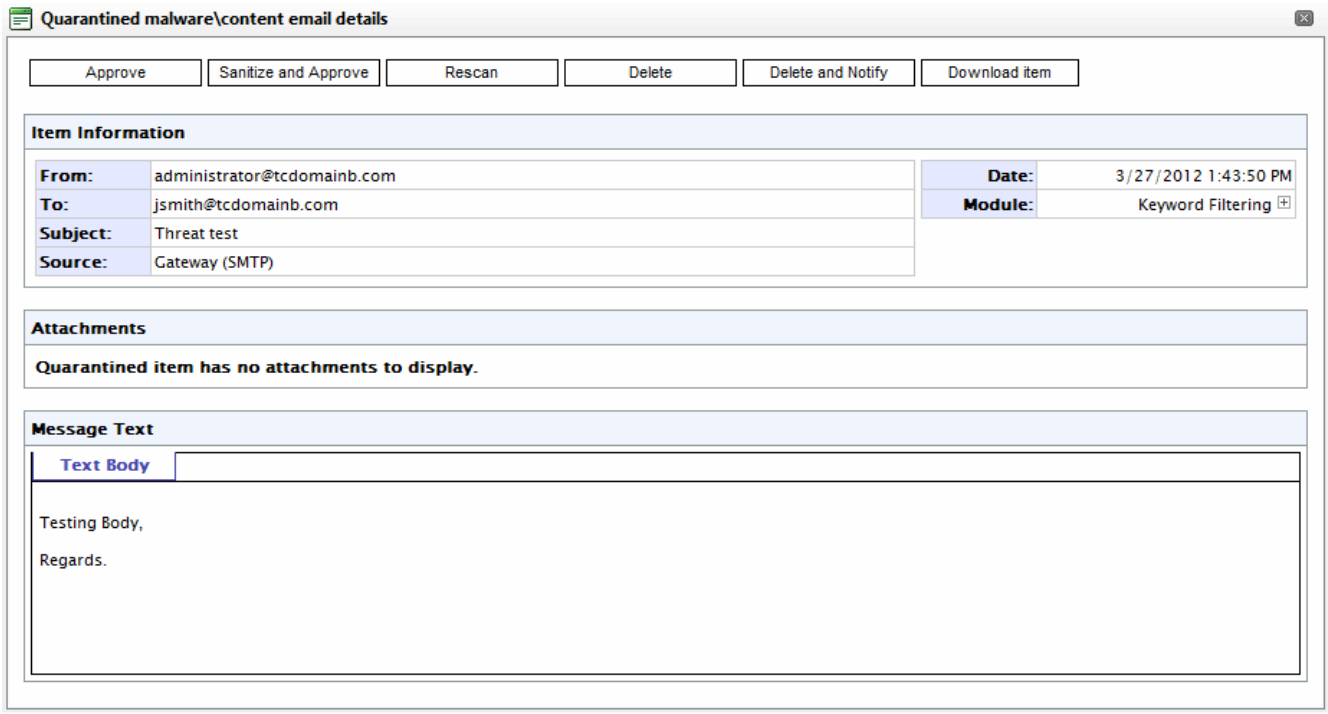
- **Malware and Content** - Emails blocked by anti-malware engines and content filtering rules.
- **Spam** - Emails blocked by anti-spam filters.

1. Choose **Malware and Content** tab or **Spam** tab to view quarantined emails for the specific quarantined email type. The results page provides the following functions and details:

Option	Description
Back	Returns you to the previous screen.
Approve	Enables you to approve a single or multiple emails. For more information, refer to Approving Quarantined Emails (page 189).
Delete	Deletes a single or multiple emails. For more information, refer to Permanently Delete Quarantined Emails (page 190).
Rescan	Rescans emails using current antivirus signatures (which may be more up to date than the antivirus signatures that quarantined the email in the first place). Select one or more emails and click **Rescan** to rescan.
Module	The module that identified the email as to be quarantined.
Reason	The reason/rule that triggered the action to quarantine the email.
Sender	The email address of the sender
Recipients	The email address of the recipient
Subject	The email subject as sent by the sender.

Option	Description
Date	The date when email was quarantined
Source	The location from where the email was quarantined
Item Source	Enables selecting a source to filter the display with. Available options are: » View all » Information Store (VSAPI) » Gateway (SMTP) » Information Store (Transport)
Page size	Enables customizing how many emails per page are currently displayed. Choose a number to view a maximum number of items per page.

2. Click a row to access the individual email details.



Screenshot 102: Quarantined Items details

From the **Quarantined Items details** page, review the email details and perform the following actions

Action	Description
Approve	Approve email. For more information, refer to Approving Quarantined Emails (page 189).
Sanitize and Approve	Sanitize email and approve. For more information, refer to Approving Quarantined Emails (page 189).
Rescan	Rescans emails using current antivirus signatures (which may be more up to date than the antivirus signatures that quarantined the email in the first place).
Delete	Deletes email. For more information, refer to Permanently Delete Quarantined Emails (page 190).
Delete and Notify	Deletes email and notifies user. For more information, refer to Permanently Delete Quarantined Emails (page 190).
Download Item	Downloads quarantined email to a location you choose in .eml format. **Warning:** **Emails in Quarantine Store may contain malicious content. Use this feature with caution.**

9.4.2 Approving Quarantined Emails

There might be instances where you might want to approve an email blocked by GFI MailEssentials. GFI MailEssentials allows the administrator to approve a quarantined email so that it is released from the Quarantine Store and delivered to its intended recipients.

To approve emails:

1. Use the search features described in the previous sections to return a list of quarantined emails.
2. Select the checkbox next to the quarantined email(s) to approve and click **Approve**.

Sanitize and Approve Emails

GFI MailEssentials also enables you to remove the item that caused the email to be quarantined and send the email to recipient.

To sanitize and approve emails:

1. Use the search features described in the previous sections to return a list of quarantined emails.
2. Click on an email to view its details.
3. Click **Sanitize and Approve**.

> **NOTE**
>
> Emails quarantined by the Information Store (VSAPI) source cannot be sanitized.

9.4.3 Permanently Delete Quarantined Emails

1. Use the search features described in the previous sections to return a list of quarantined emails
2. Select the checkbox next to the quarantined email(s) and click **Delete**.

Delete Quarantined Emails and notify user

The Delete and Notify feature enables notifying recipients when deleting emails from quarantine.

To delete and notify recipients:

1. Use the search features described in the previous sections to return a list of quarantined emails.
2. Click on an email to view its details.
3. Click **Delete and Notify**.

9.5 Quarantine RSS Feeds

RSS (Really Simple Syndication) is a protocol used to distribute frequently updatable content or feeds (for example, news items) with its subscribers. An RSS Feed Reader is required by subscribers to view RSS feeds. RSS feeds usually include a summary of the content and a link to view the full article.

To facilitate the monitoring of quarantined emails, RSS feeds can be used. The GFI MailEssentials Quarantine RSS feed displays quarantined emails for review and enables users to approve or delete quarantined emails.

NOTE

GFI MailEssentials Quarantine RSS feeds can be used on most RSS Feed Readers. For a list of freely available RSS Feed Readers that were tested with GFI MailEssentials Quarantine RSS feeds refer to:

http://kbase.gfi.com/showarticle.asp?id=KBID002661

Topics in this chapter:

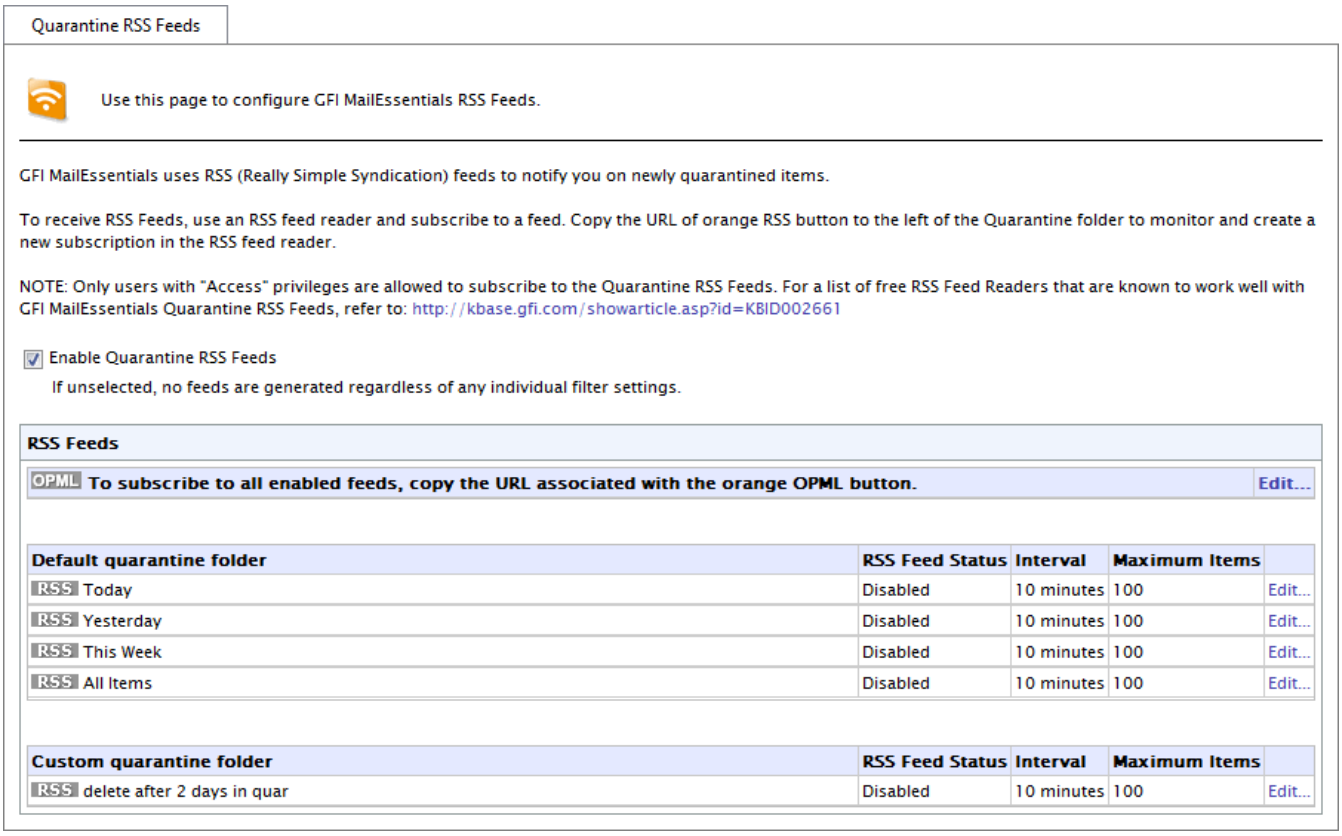
9.5.1 Enabling Quarantine RSS Feeds 191

9.5.2 Subscribing to Quarantine RSS feeds 192

9.5.3 Securing access to the GFI MailEssentials Quarantine RSS feeds 192

9.5.1 Enabling Quarantine RSS Feeds

1. Navigate to **GFI MailEssentials > Quarantine > Quarantine RSS Feeds.**


Quarantine RSS Feeds
Use this page to configure GFI MailEssentials RSS Feeds.
GFI MailEssentials uses RSS (Really Simple Syndication) feeds to notify you on newly quarantined items.
To receive RSS Feeds, use an RSS feed reader and subscribe to a feed. Copy the URL of orange RSS button to the left of the Quarantine folder to monitor and create a new subscription in the RSS feed reader.
NOTE: Only users with "Access" privileges are allowed to subscribe to the Quarantine RSS Feeds. For a list of free RSS Feed Readers that are known to work well with GFI MailEssentials Quarantine RSS Feeds, refer to: http://kbase.gfi.com/showarticle.asp?id=KBID002661
Enable Quarantine RSS Feeds
If unselected, no feeds are generated regardless of any individual filter settings.
RSS Feeds
OPML To subscribe to all enabled feeds, copy the URL associated with the orange OPML button.
Edit...
Default quarantine folder
RSS Feed Status
Interval
Maximum Items
RSS Today
Disabled
10 minutes
100
Edit...
RSS Yesterday
Disabled
10 minutes
100
Edit...
RSS This Week
Disabled
10 minutes
100
Edit...
RSS All Items
Disabled
10 minutes
100
Edit...
Custom quarantine folder
RSS Feed Status
Interval
Maximum Items
RSS delete after 2 days in quar
Disabled
10 minutes
100
Edit...

Screenshot 103: Quarantine RSS feeds

2. Select the **Enable Quarantine RSS Feeds** checkbox.
3. From the **RSS Feeds** area, click **Edit** to the right of the quarantine search folder for which to enable RSS feeds.

4. Select **Enable Quarantine RSS feeds on this folder** checkbox.
5. Specify the refresh interval in minutes in the **Refresh feed content every** text box. The default value is 10 minutes.
6. Specify the maximum number of items you want the feed to include in the **Feed should contain at most** text box. The default value is 100 items.

> **NOTE**
>
> You can change the URL of an RSS feed by clicking **Reset Feed URL**. To change the URL of all enabled RSS feeds, click **Edit** to the right of the **OPML** entry and click **Reset all the URLs**. When changing URL's, ensure to update all present subscriptions accordingly.
>
> Reset feed url should be done in case of unauthorized access

7. Click **Apply**.

9.5.2 Subscribing to Quarantine RSS feeds

Subscribing to all enabled Quarantine RSS feeds

1. Navigate to **GFI MailEssentials > Quarantine >Quarantine RSS Feeds**.

2. In the RSS Feeds area, right-click on OPML icon and click **Copy Shortcut** to copy the RSS feed URL.
3. Use the copied URL in your RSS Feed Reader application to create a new RSS feed subscription.

Subscribing to a search folder Quarantine RSS feed

To subscribe to an RSS feed of a default or custom search folder:

1. Navigate to **GFI MailEssentials > Quarantine >Quarantine RSS Feeds**.

2. In the RSS Feeds area, right-click on RSS icon next to the search folder to subscribe to and click **Copy Shortcut** to copy the RSS feed URL.
3. Use the copied URL in your RSS Feed Reader application to create a new RSS feed subscription.

9.5.3 Securing access to the GFI MailEssentials Quarantine RSS feeds

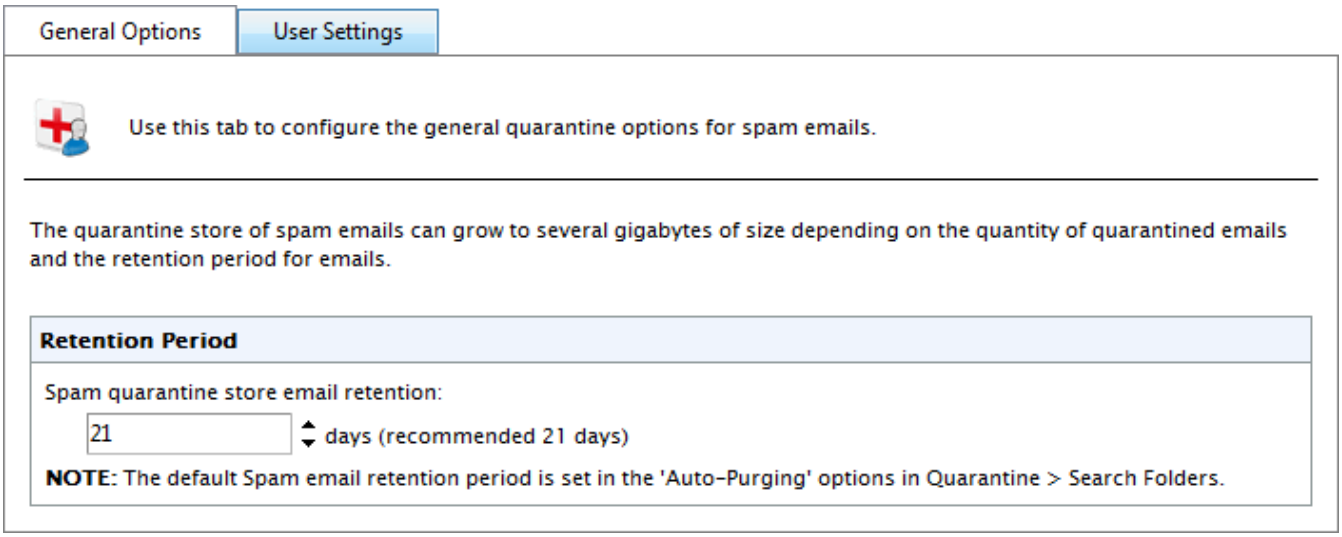
Configure who can subscribe to the quarantine RSS feeds from the Access Control node in GFI MailEssentials Configuration. For more information, refer to Access Control (page 225).

9.6 Quarantine Options

Use the Quarantine Options to configure Quarantined Spam retention, User Reporting and Quarantined Malware non-existent user setup.

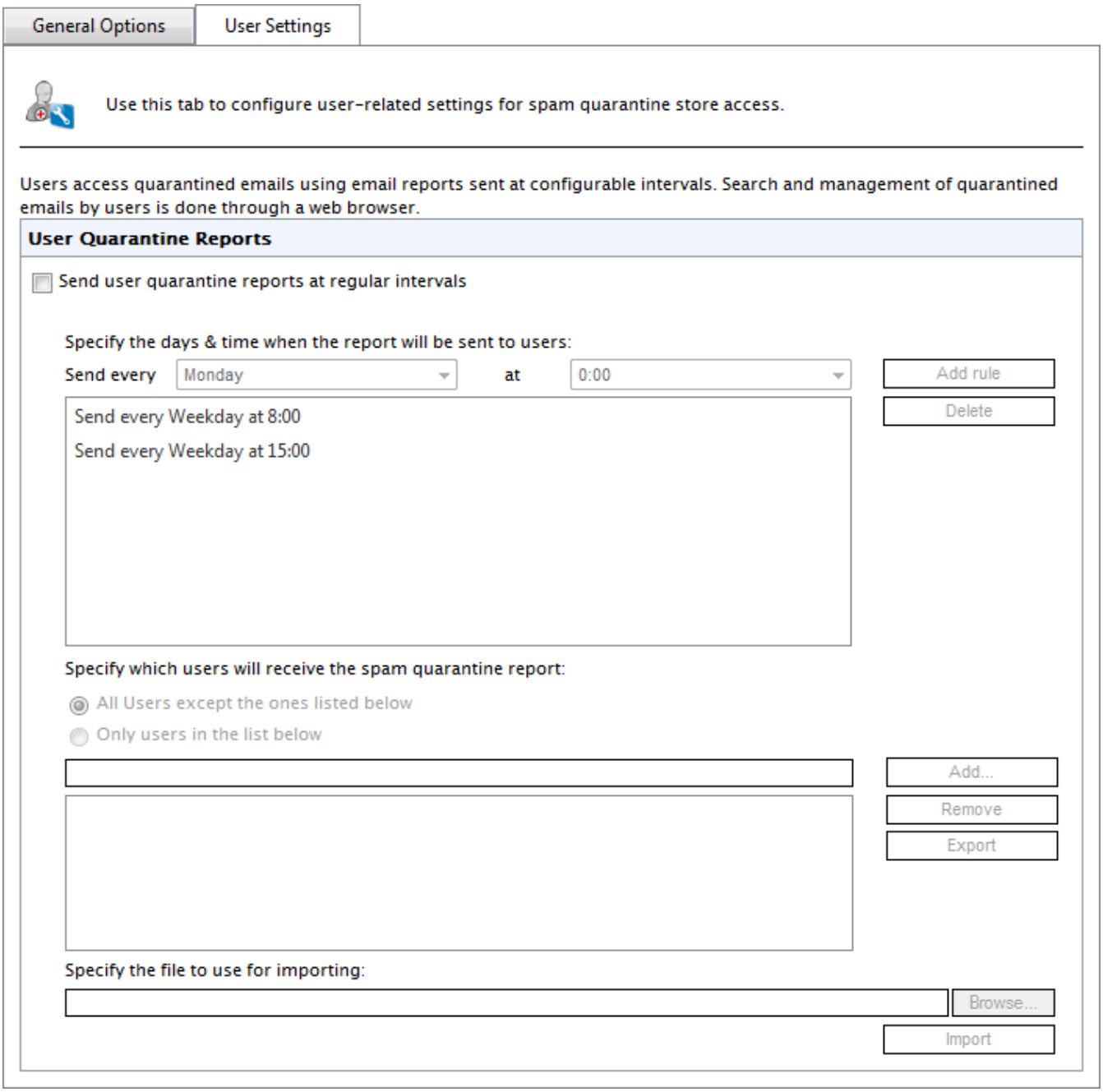
9.6.1 Spam Options

1. Navigate to **Quarantine > Quarantine Options > Spam Options**.


General Options
User Settings
Use this tab to configure the general quarantine options for spam emails.
The quarantine store of spam emails can grow to several gigabytes of size depending on the quantity of quarantined emails and the retention period for emails.
Retention Period
Spam quarantine store email retention:
21
days (recommended 21 days)
NOTE: The default Spam email retention period is set in the 'Auto-Purging' options in Quarantine > Search Folders.

Screenshot 104: Spam Options - General Options tab

2. From the **General Options** tab change or confirm the **Spam quarantine store email retention** period.
3. Click **User Settings** tab.


General Options
User Settings
Use this tab to configure user-related settings for spam quarantine store access.
Users access quarantined emails using email reports sent at configurable intervals. Search and management of quarantined emails by users is done through a web browser.
User Quarantine Reports
Send user quarantine reports at regular intervals
Specify the days & time when the report will be sent to users:
Send every
Monday
at
0:00
Add rule
Delete
Send every Weekday at 8:00
Send every Weekday at 15:00
Specify which users will receive the spam quarantine report:
All Users except the ones listed below
Only users in the list below
Add...
Remove
Export
Specify the file to use for importing:
Browse...
Import

Screenshot 105: Spam Options - User Settings tab

4. Select **Send user quarantine reports at regular intervals** to enable sending of User quarantine reports.

> **NOTE**
>
> User quarantine reports are emails sent to users on a regular basis with a list of blocked spam for that user. Using this list, users can check and approve any legitimate emails. Email blocked by the Malware and Content Filtering filters are not shown in these emails.

5. Configure the frequency at which report will be sent. To add to the preset schedule, select a date and time and click **Add rule.** Select an existing date and time and click **Delete** to delete

selected date/time.

6. Configure the users that will receive the Quarantined Spam reports. Select **All Users except the ones listed below** or **Only users in the list below** and provide the email address of the users to include or exclude.

> **NOTE**
>
> Click **Browse** to select a file with a list of email addresses to import and click **Import**.

7. Click **Apply**.

9.6.2 Malware Options

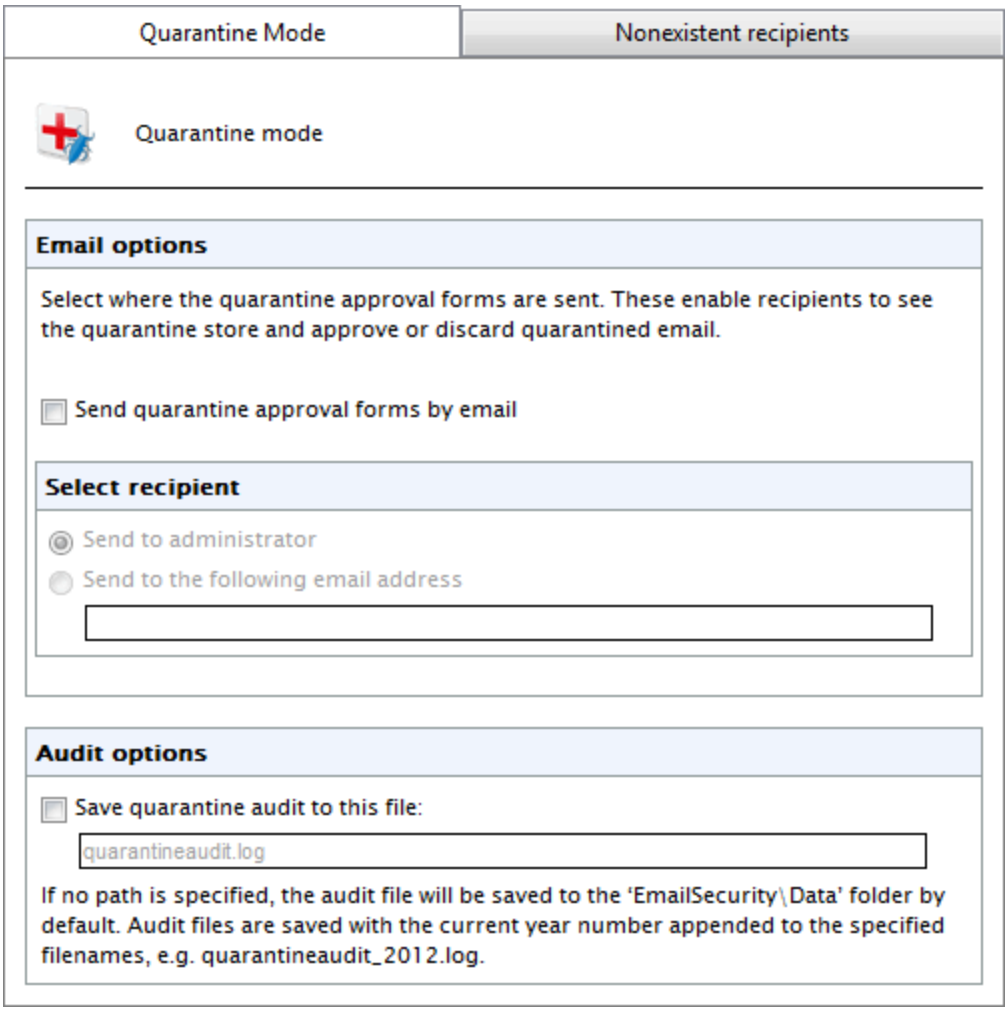
GFI MailEssentials can also be configured to notify the administrator or authorized users via email (Quarantine Action Form) whenever an email is quarantined.

The Quarantine Approval Form contains details related to the quarantined email including the reason why it was blocked and any attachments that were included in the email. The administrator can then action the quarantined email (for example, approve the email) directly from the email client.

> **NOTE**
>
> To automatically purge emails older than a specific number of days, create a new search folder and set the Auto-purging feature to purge emails after a number of days. For more information, refer to Using the Search Folders node to auto-purge quarantined emails (page 187).

Enabling Quarantine Approval Forms

1. Navigate to **Quarantine > Quarantine Options > Malware Options**.


Quarantine Mode
Nonexistent recipients
Quarantine mode
Email options
Select where the quarantine approval forms are sent. These enable recipients to see the quarantine store and approve or discard quarantined email.
Send quarantine approval forms by email
Select recipient
Send to administrator
Send to the following email address
Audit options
Save quarantine audit to this file:
quarantineaudit.log
If no path is specified, the audit file will be saved to the 'EmailSecurity\Data' folder by default. Audit files are saved with the current year number appended to the specified filenames, e.g. quarantineaudit_2012.log.

Screenshot 106: Quarantine Mode

2. From **Quarantine Mode** tab, select **Send quarantine approval forms by email** checkbox to enable the sending of Quarantine Approval Forms.
3. From the **Select recipient** area, specify the recipient of the Quarantine Approval Forms:

Option	Description
Send to administrator	Sends Quarantine Approval Forms to the administrator as configured in **General Settings** node. For more information, refer to Administrator email address (page 219).
Send to the following email address	Sends Quarantine Approval Forms to another email address. Key in the recipient in the text box provided.

4. Optional - Select **Save quarantine audit to this file** and configure a filename where to save a copy of the quarantine log.
5. Click **Apply.**

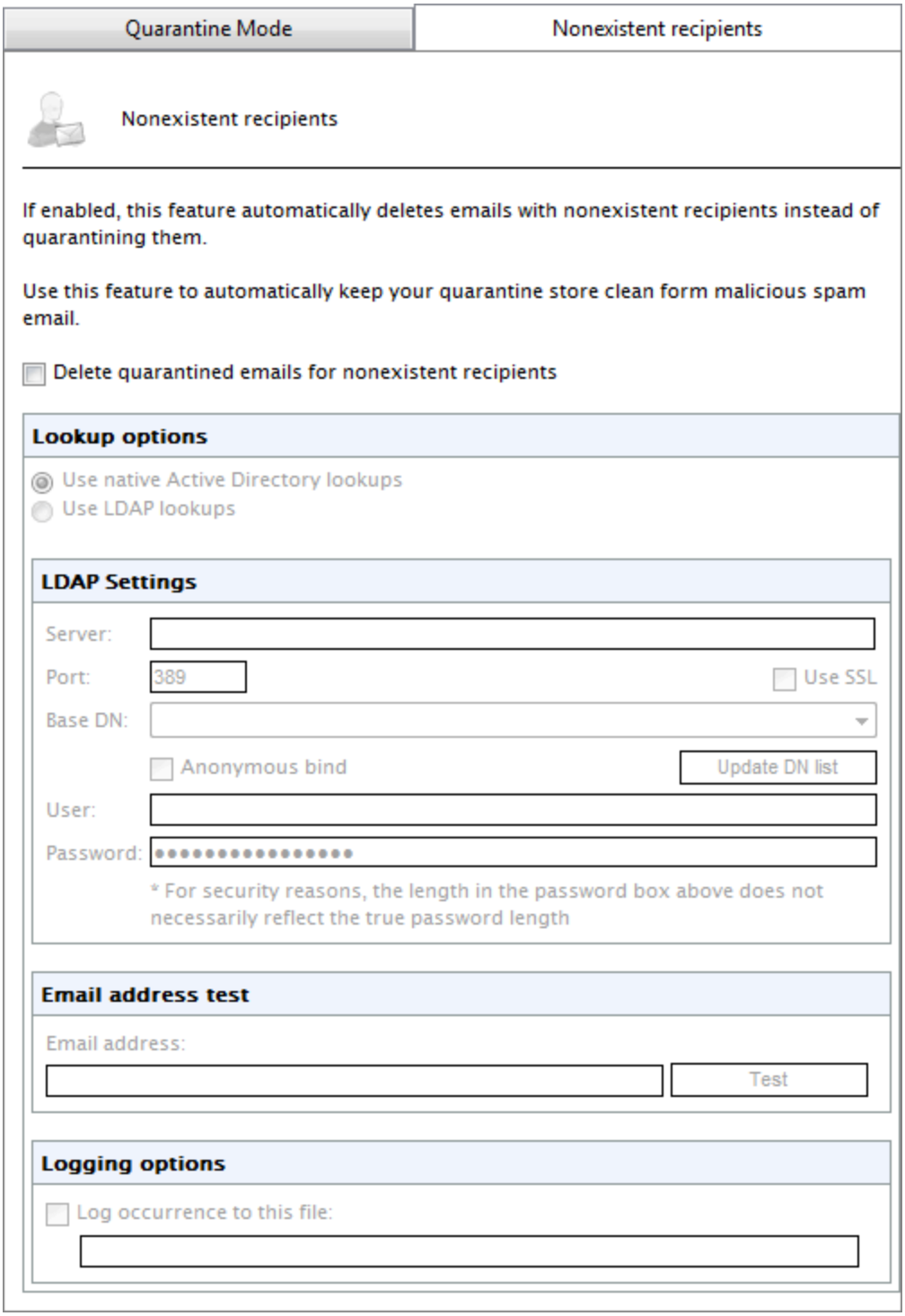
Nonexistent Recipients

The GFI MailEssentials Nonexistant recipients feature scans emails for non-existing local email addresses before these are stored to the Quarantine Store. If an email contains non-existing local email addresses, it is permanently deleted. This reduces the number of emails for administrative reviewing.

Configuring Nonexistent Recipients

The Nonexistent Recipients filter requires access to the list of local addresses. This is done either via Active Directory or if communication with Active Directory is not possible, via an LDAP server.

1. Navigate to **Quarantine > Quarantine Options > Malware Options**.



Screenshot 107: Nonexistent Recipients

2. From **Nonexistent Recipients** tab, select **Enable Nonexistent Recipients protection** checkbox.
3. Select the user lookups method to use:

Option	Description
Use native Active Directory lookups	Select this option if GFI MailEssentials is installed in Active Directory mode and has access to ALL users on Active Directory. Skip to step 8. **NOTE** When GFI MailEssentials is installed in Active Directory user mode on a DMZ, the AD of a DMZ usually does not include all the network users (email recipients). In this case configure GFI MailEssentials to use LDAP lookups. **NOTE** WhenGFI MailEssentials is behind a firewall, this feature might not be able to connect directly to the internal Active Directory because of Firewall settings. Use LDAP lookups to connect to the internal Active Directory of your network and ensure to enable default port 389 on your Firewall.
Use LDAP lookups	Select this option when GFI MailEssentials is installed in SMTP mode and/or when GFI MailEssentials does not have direct access to the full list of users.

4. Specify the LDAP server name or IP address in the **Server** text box.

> **NOTE**
>
> In an Active Directory environment, the LDAP server is typically the Domain Controller or Global Catalog.

5. Specify the port number, default 389, in the **Port** text box. If connection to the LDAP server is via SSL, select **Use SSL** and the default port changes to 636.

> **NOTE**
>
> Ensure that the port is enabled from the Firewall.

6. Click **Update DN list** to populate the **Base DN** list and select the Base DN (that is, the top level in the Active Directory hierarchy).
7. If your LDAP server requires authentication specify the **User** and **Password**. Alternatively, if no authentication is required, select **Anonymous bind**.
8. Test your configuration settings by specifying a valid email address in the **Email address** box and click **Test**. If the email address is not found, review the configuration settings.
9. To log Nonexistent Recipient activity to a log file, select **Log occurrence to this file** and specify path and file name (including .txt extension) to a custom location on disk where to store the log file. Alternatively specify the file name only (including .txt extension) and the log file will be stored in the following default location

```
<GFI MailEssentials installation
path>\GFI\MailEssentials\\EmailSecurity\Logs\<filename>.txt
```

10. Click **Apply**.

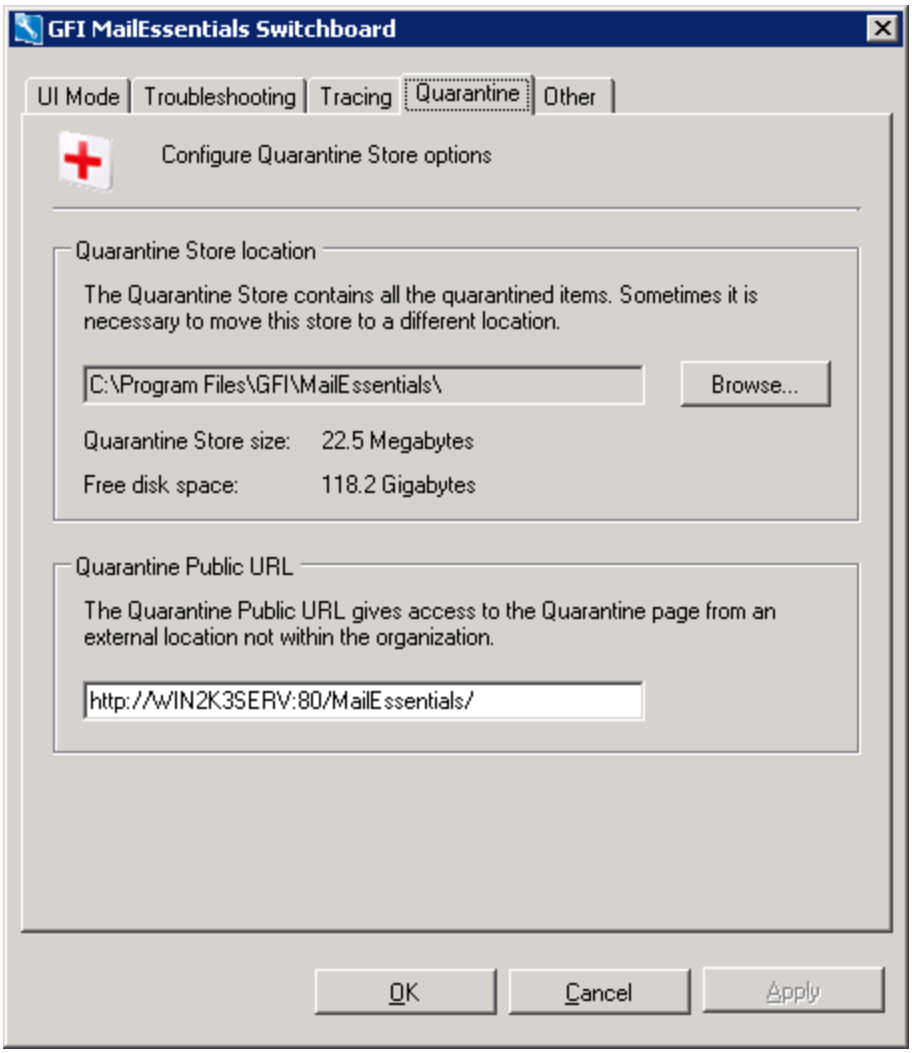
9.7 Quarantine Store Location and Public URL

Use the GFI MailEssentials Switchboard to configure the Quarantine Store location and the Quarantine Public URL.

The Quarantine Store location is the Quarantine Store location where quarantined emails are stored. By default, this is located in the GFI MailEssentials installation path. This might however need to be moved to an alternate location in cases where, for example, you might be running out of disk space.

The Quarantine Public URL provides access to the Quarantine Page from an external location. By default, this is based on the GFI MailEssentials IIS Virtual directory settings you provided during installation. This however might need to be changed if you are sending quarantine digest emails or notifications that are accessed outside of the internal network. When this is the case, the URL should be changed to be reached through Internet.

1. Launch the GFI MailEssentials Switchboard from **Start > Programs > GFI MailEssentials > Switchboard**.



Screenshot 108: Quarantine Store location and Public URL

2. From **Quarantine** tab, click **Browse** to select an alternate location for the Quarantine Store.

IMPORTANT

Ensure that the disk partition where the Quarantine Store is saved has sufficient disk space. Spam emails will not be quarantined if the free disk space is less than 512 MB. On reaching 512 MB, email quarantine operation will stop and spam will be tagged and delivered to recipients' mailboxes until free disk space increases to more than 512 MB

3. Provide an alternate URL as the URL to use to access the quarantine from an external location outside your organization,

4. Click **OK** to save setup.

10 Email Management

GFI MailEssentials includes a number of tools that facilitate management of incoming and outgoing emails.

Topics in this chapter:

10.1 Disclaimers 201
10.1.1 Configuring Disclaimers 201
10.1.2 Disabling and enabling disclaimers 205
10.2 Auto-Replies 205
10.2.1 Configuring auto-replies 206
10.3 List Server 208
10.3.1 Creating a newsletter or discussion list 208
10.3.2 Using Newsletters/Discussions 210
10.3.3 Configuring advanced newsletter/discussion list properties 211
10.4 Mail Monitoring 215
10.4.1 Enabling/Disabling email monitoring 215
10.4.2 Configure email monitoring 216

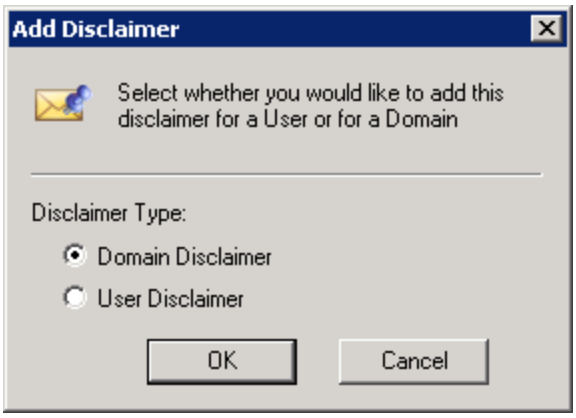
10.1 Disclaimers

Disclaimers are standard content added to the bottom or top of outbound email for legal and/or marketing reasons. These assist companies in protecting themselves from potential legal threats resulting from the contents of an email and to add descriptions about the products/services offered.

- Configuring Disclaimers
- Disabling\Enabling Disclaimers

10.1.1 Configuring Disclaimers

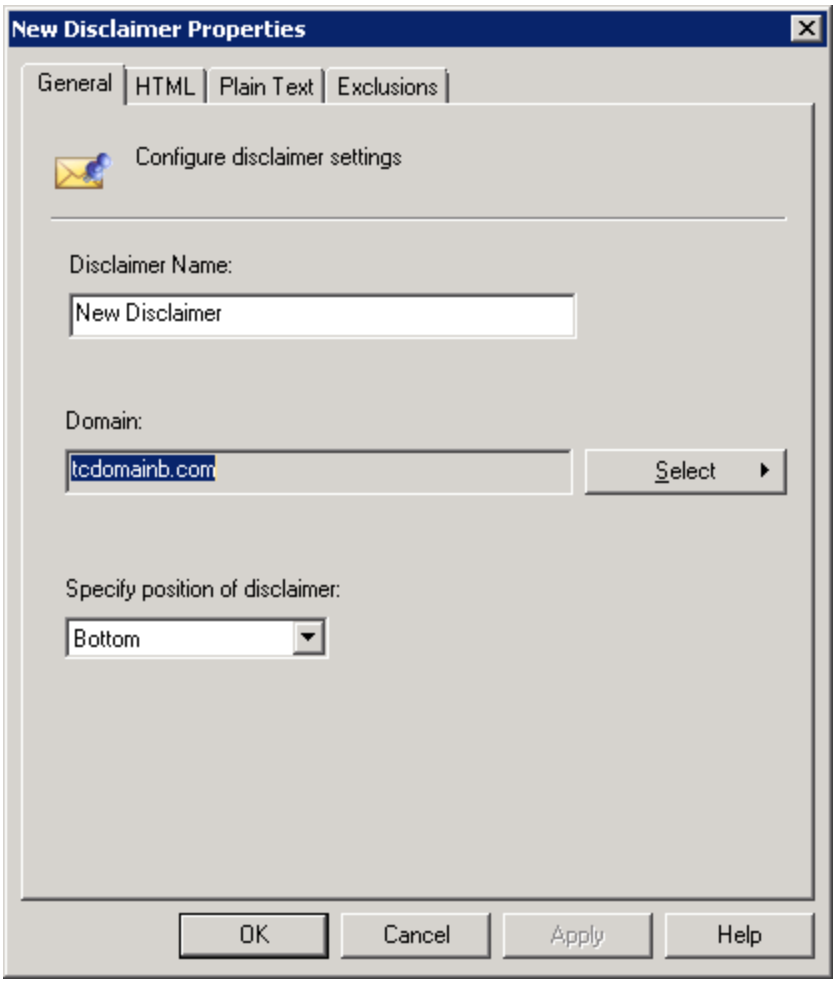
1. Click **Start > All Programs > GFI MailEssentials > Email Management Tools** to load Email Management Tools.
2. Select the **Disclaimers** node and double click a disclaimer to edit settings. Alternatively, to create a new disclaimer, right click **Disclaimers** node, and select **New > Disclaimer**.



Screenshot 109: Choose Disclaimer type

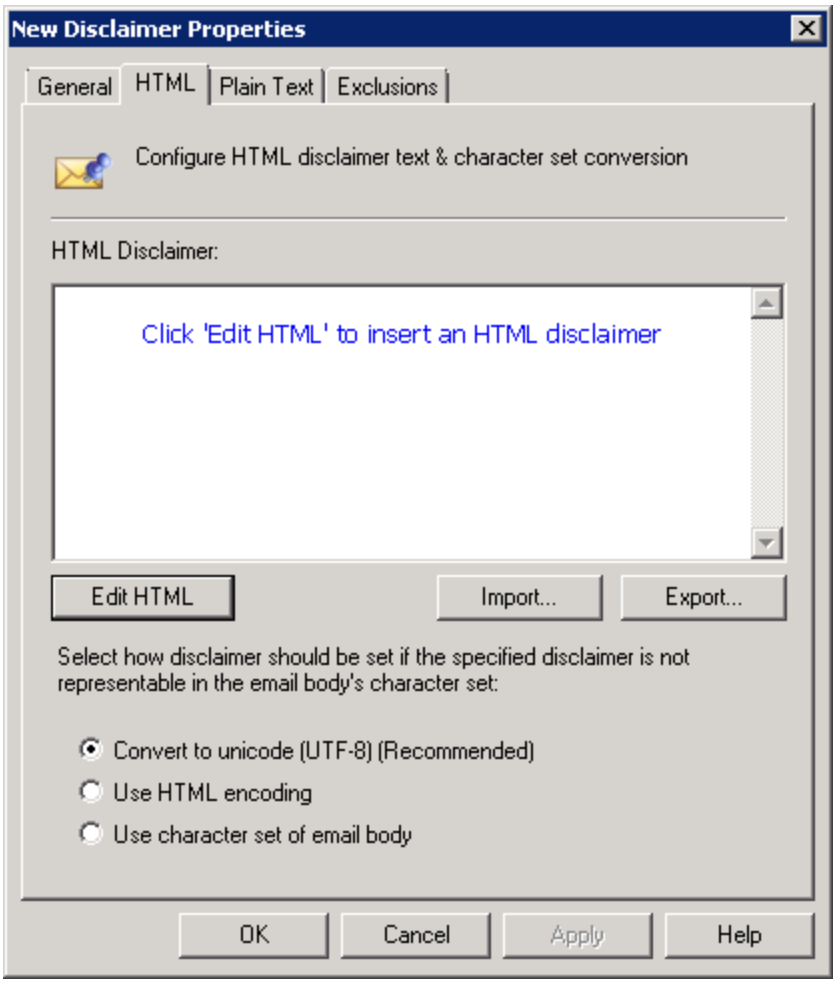
3. Select:

Option	Description
Domain Disclaimer	Choose the domain from the list of configured domains. All emails sent from that domain will have the disclaimer added.
User Disclaimer	Specify a user or group of users, to whom the disclaimer is added for outbound emails. If GFI MailEssentials is in Active Directory mode, pick users or groups of users directly from Active Directory; else specify the SMTP email address of the user.



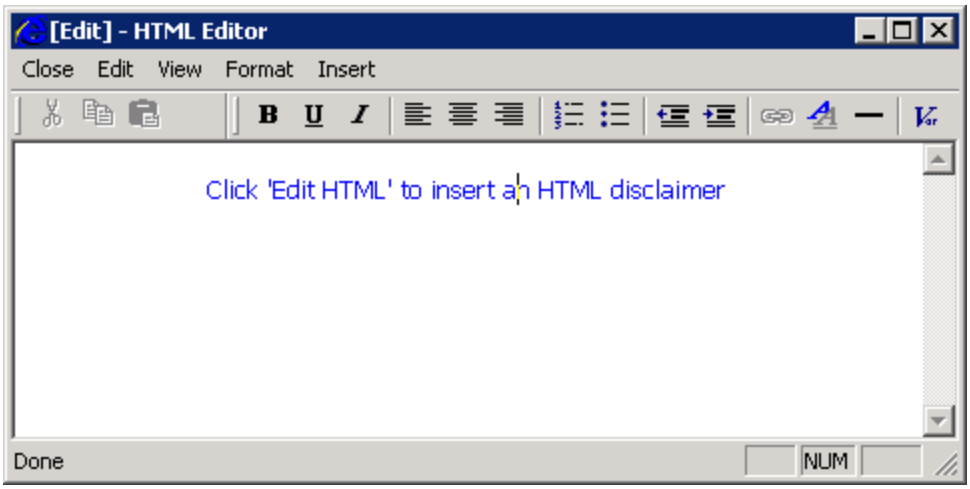
Screenshot 110: New Disclaimer general properties

4. In the **General** tab, key in **Disclaimer Name**, click **Select** to change the domain or user. Select **Top** or **Bottom** option to configure if disclaimer should be located at the top or bottom of the email.



Screenshot 111: HTML Disclaimer

5. To add a disclaimer in HTML format, select the **HTML** tab. Click **Edit HTML** to launch the HTML disclaimer editor and edit the HTML disclaimer text.



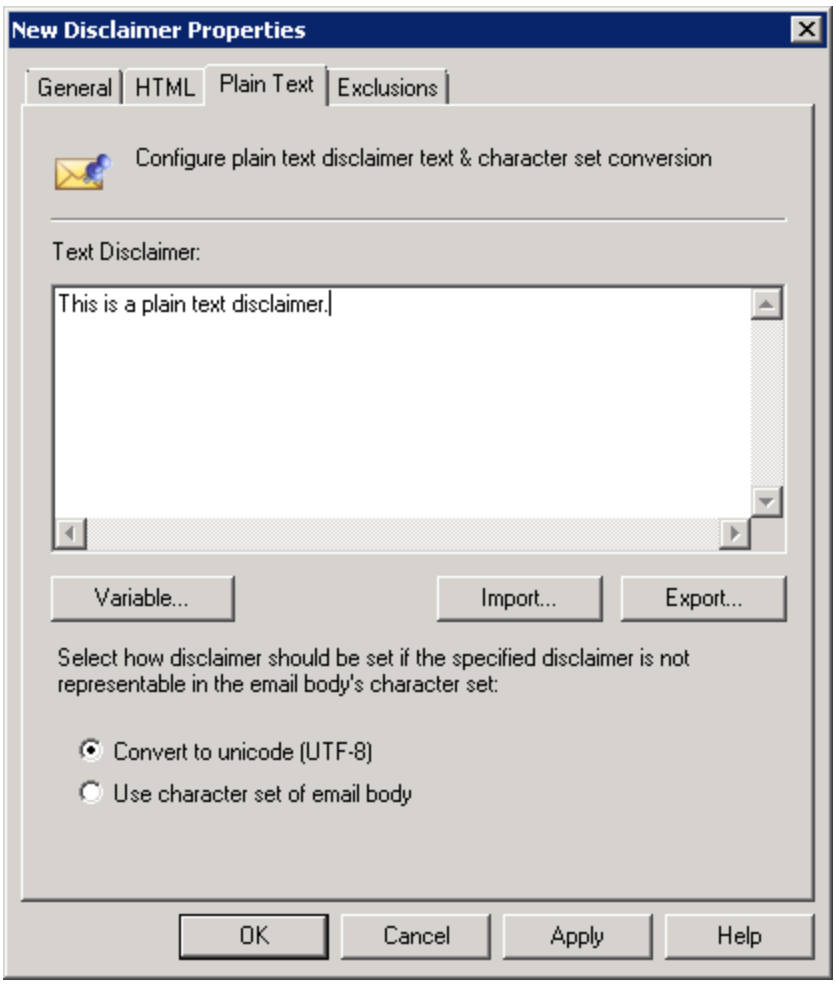
Screenshot 112: HTML disclaimer editor

6. To add variables in disclaimer, navigate to **Insert > Variable…**. The variables that can be added are email fields or Active Directory fields. Select the variable to add and click **OK**.

> **NOTE**
>
> The recipient display name and email address variables will only be included if the email is sent to a single recipient. If emails are sent to multiple recipients, the variables are replaced with 'recipients'.

7. Click **Close** when finished editing the HTML disclaimer.
8. Import or export an HTML disclaimer in .htm or .html format using the **Import** and **Export** buttons.
9. Specify the encoding for the HTML disclaimer if the email body's character set is not HTML:

Option	Description
Convert to Unicode	Convert both email body and disclaimers to Unicode so that both are properly displayed. (Recommended)
Use HTML encoding	Use to define character sets for email body and disclaimer.
Use character set of the email body	Disclaimer is converted to the email body character set. **NOTE** If selected, some disclaimer text might not display properly.



Screenshot 113: Plain text disclaimer

10. Select **Plain Text** tab and insert the text to include for use in plain text emails directly into the **Text Disclaimer** field.

11. Optionally add variables in disclaimer by clicking **Variable…**. The variables that can be added are email fields (sender name, recipient email address, etc…) or Active Directory fields (name, title, telephone numbers, etc..). Select the variable to add and click **OK**.

> **NOTE**
>
> The recipient display name and email address variables will only be included if the email is sent to a single recipient. If emails are sent to multiple recipients, the variables are replaced with 'recipients'.

12. Specify the encoding to be used for the plain text disclaimer if the email body's character set is not plain text:

Option	Description
Convert to unicode	Converts both email body and disclaimers to Unicode so that both are properly displayed
Use character set of the email body	Disclaimer is converted to the email body's character set **NOTE** If this option is selected, some of the disclaimer text might not be displayed properly.

13. Import or export a plain text disclaimer format using the **Import** and **Export** buttons.

14. From the **Exclusions** tab, specify any senders or recipients for whom not to apply this disclaimer. Click **Add** and specify the **User** or **Email Address** to exclude.

> **NOTE**
>
> All recipients must be included in the exclusion list to not add a disclaimer in the email.

15. Click **OK** to save settings.

10.1.2 Disabling and enabling disclaimers

By default, disclaimers are automatically enabled. To disable or enable a disclaimer:

1. Click **Start > All Programs > GFI MailEssentials > Email Management Tools** to load Email Management Tools.

2. Select **Disclaimers** node and right click the disclaimer.

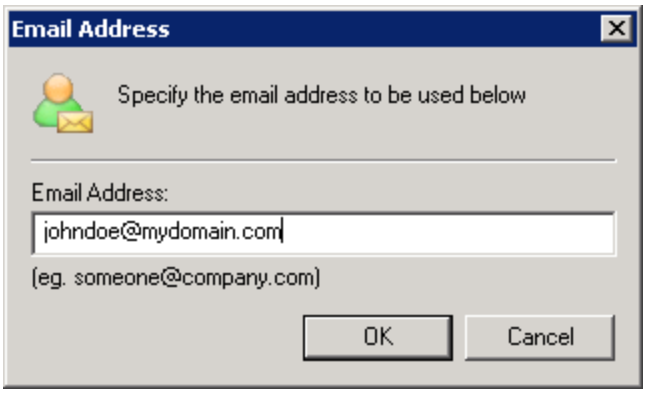
3. Select **Disable** or **Enable** to perform the desired action.

10.2 Auto-Replies

Auto-replies enable the sending of automated replies to specific inbound emails. A different auto-reply for each email address or subject can be specified. Variables can also be used in an auto-reply to personalize emails.

10.2.1 Configuring auto-replies

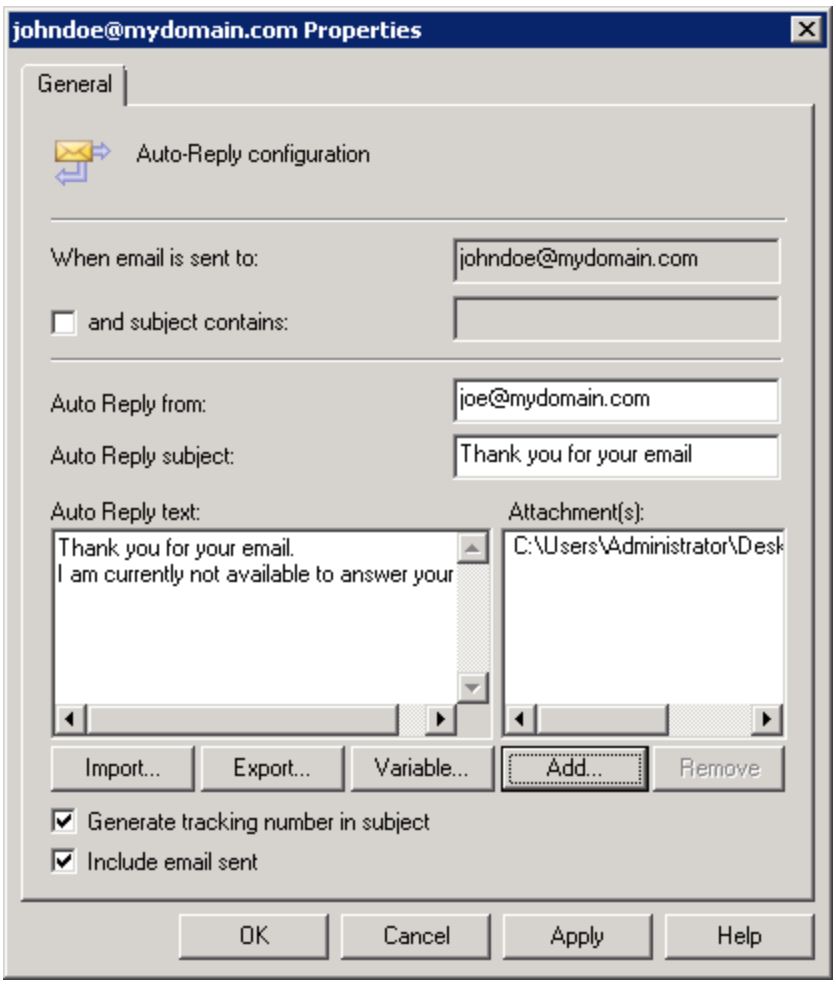
1. Click **Start > All Programs > GFI MailEssentials > Email Management Tools** to load Email Management Tools.
2. Right click **Email management > Auto-Replies** node and select **New > Auto-Reply**.



Screenshot 114: Creating a new auto reply

3. Key in the email address that sends auto-replies when receiving emails, and click **OK**.

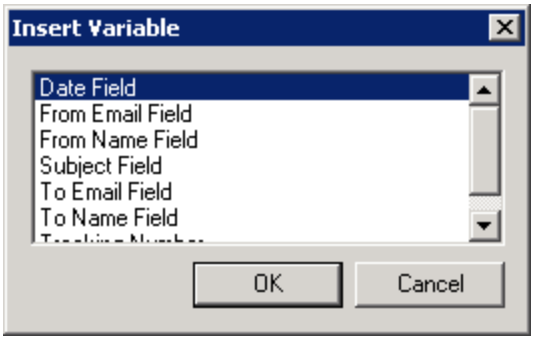
Example - If 'sales@master-domain.com' is used, senders sending to this email address will receive an auto reply.



Screenshot 115: Auto-reply properties

4. Check **and subject contains:** checkbox to enable auto replies for emails containing specific text in the subject field.
5. In the **Auto Reply from:** field, specify an email address in case where an auto-reply is required from a different email address other than the email address to which the inbound email was addressed to.
6. In the **Auto Reply subject** field, specify the subject of the auto reply email.
7. In **Auto Reply text**, specify the text to display in the auto reply email.

> **NOTE**
>
> Import auto reply text from a text file via the **Import...** button.



Screenshot 116: Variables dialog

8. Click **Variable...** to personalize auto-replies using variables. Select variable field to insert and click **OK**. Available variables are:

Option	Description
Date Field	Inserts the email sent date.
From Email Field	Insert sender email address.
From Name Field	Inserts the display name of the sender.
Subject Field	Inserts email subject.
To Email Field	Inserts the recipient's email address.
To Name Field	Inserts the recipient's display name.
Tracking Number	Inserts tracking number (if generated).

9. Click **Add...** and select any attachments to send with the auto-reply email. Remove attachments using **Remove**.
10. Select **Include email sent** option to quote the inbound email in auto reply.
11. Select **Generate tracking number** in subject to enable the generation of tracking numbers in the auto replies.

> **NOTE**
>
> This feature enables, for example, customers to reply quoting a tracking number that enables staff to track emails in a more coherent manner.

NOTE

By default, tracking numbers are generated using the following format: `ME_YYMMDD_nnnnnn`

Where:

- `ME` - GFI MailEssentials tag.
- `YYMMDD` - Date in year, month and date format.
- `nnnnnn` - automatically generated tracking number.

12. Click **OK** button to finalize settings.

10.3 List Server

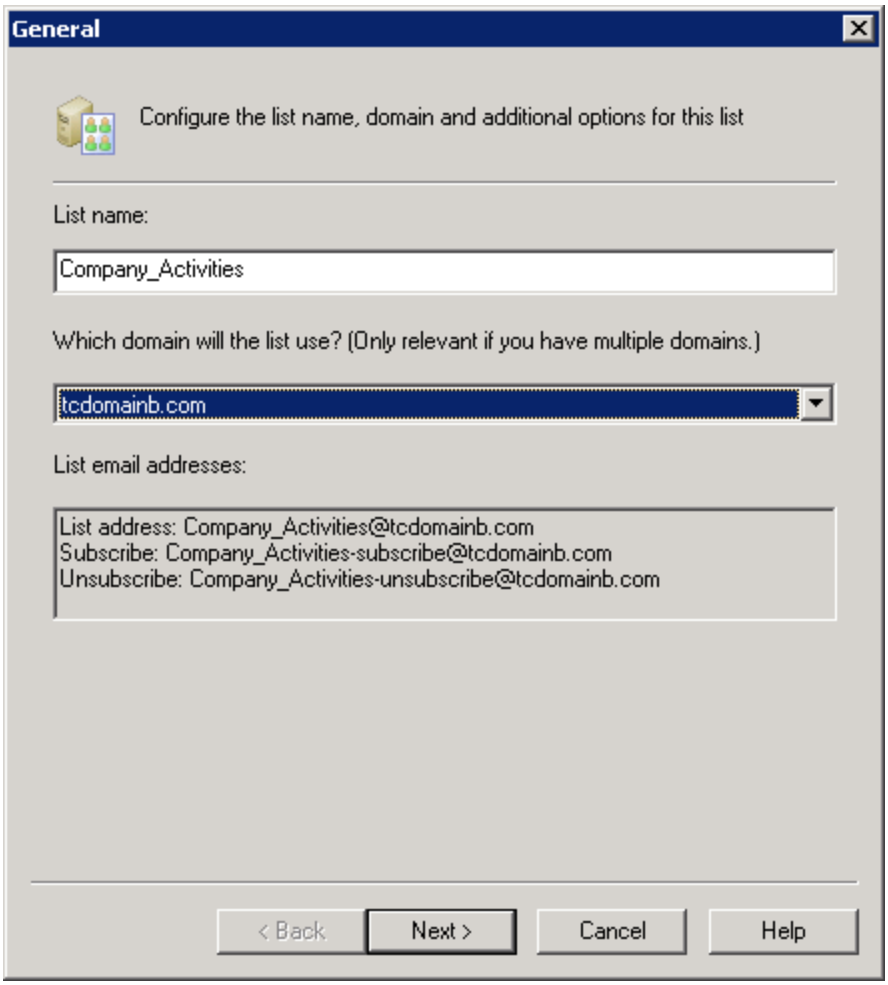
List servers enable the creation of two types of distributions lists:

1. A newsletter subscription list - Used for creating subscription lists for company or product newsletters, to which users can either subscribe or unsubscribe.

2. A discussion list - Enables groups of people to hold discussions via email, with each member of the list receiving the email that a user sends to it.

10.3.1 Creating a newsletter or discussion list

1. Click **Start > All Programs > GFI MailEssentials > Email Management Tools** to load Email Management Tools.
2. Right-click **Email Management > List Server** node and select **New > Newsletter** or **Discussion List**



Screenshot 117: Creating a new list

3. In the **List name:** field, key in a name for the new list and select a domain for the list (only if you have multiple domains). Click **Next** to continue setup.
4. Select **Microsoft Access** or **Microsoft SQL Server/MSDE** as database and from the **Database type** group select if GFI MailEssentials should create a new database or connect to an existing database. Click **Next** to continue.

> **NOTE**
>
> For lists of up to 5000 members, you can use Microsoft Access as a backend.

> **NOTE**
>
> To create a new database, select **Automatic** option.

5. Configure the database type selected to store the newsletter/discussion subscribers list. The available options are:

Option	Description
Microsoft Access with **Automatic Option**	Key in the location where the new database is stored in the File edit box.

Option	Description
Microsoft Access with **Existing Option**	In the File field specify the path to your existing Microsoft Access database that contains the newsletter/discussion subscribers. From the Table drop down list select the table where the subscribers list is stored.
Microsoft SQL Server with **Automatic Option**	Specify SQL server name, logon credentials and database used to store newsletter/discussion subscribers list.
Microsoft SQL with **Existing Option**	Specify SQL server name, logon credentials and select the database and table where subscribers list is stored.

6. For all database types with the Automatic option, click **Finish** button to end the wizard, or click **Next** to continue setup.

7. If you are configuring an existing Microsoft SQL Server, set up the connection to the Microsoft SQL Server. If configuring a Microsoft Access Database, configure the path to a file and select a table within the Microsoft Access Database to use.

8. Select a variable from the **Variables** list and the corresponding **Database Field** option and click **Map Field** button to Map the required fields with the custom fields found in the database. Click **Finish** to finalize your configuration. The fields to map are:

Variable	Description
[FirstName_To]	Map to a string field containing the first name of a subscriber.
[LastName_To]	Map to a string field containing the last name of a subscriber.
[Company]	Map to a string field containing the company name of a subscriber.
[Email_To]	Map to a string field containing the email address of a subscriber.
[Unsubscribe]	Map to an integer (or Boolean) value field which is used to define whether the user is subscribed to the list or not.

9. Customize your newly created list. For more information, refer to Configuring advanced newsletter/discussion list properties (page 211).

10.3.2 Using Newsletters/Discussions

After creating a newsletter/discussion list, users must subscribe to be part of the list.

Action	Description
Subscribing to list	Ask users to send an email to `<newslettername>-subscribe@yourdomain.com`
Completing subscription process	On receiving the request, list server sends a confirmation email back. Users must confirm their subscription via a reply email to be added as a subscriber. **NOTE** The confirmation email is a requirement and cannot be turned off.
Sending a newsletter/discussion post	Members with permissions to send email to the list are required to send the email to the newsletter list mailing address: `<newslettername>@yourdomain.com`
Unsubscribing from list	To unsubscribe from the list, users must send an email to: `<newslettername>-unsubscribe@yourdomain.com`

To enable users to easily subscribe to newsletters, add a web form asking for name and email address and automatically generate an email where the sender is the email address of the new user and the recipient is:

`<newslettername>-subscribe@yourdomain.com`

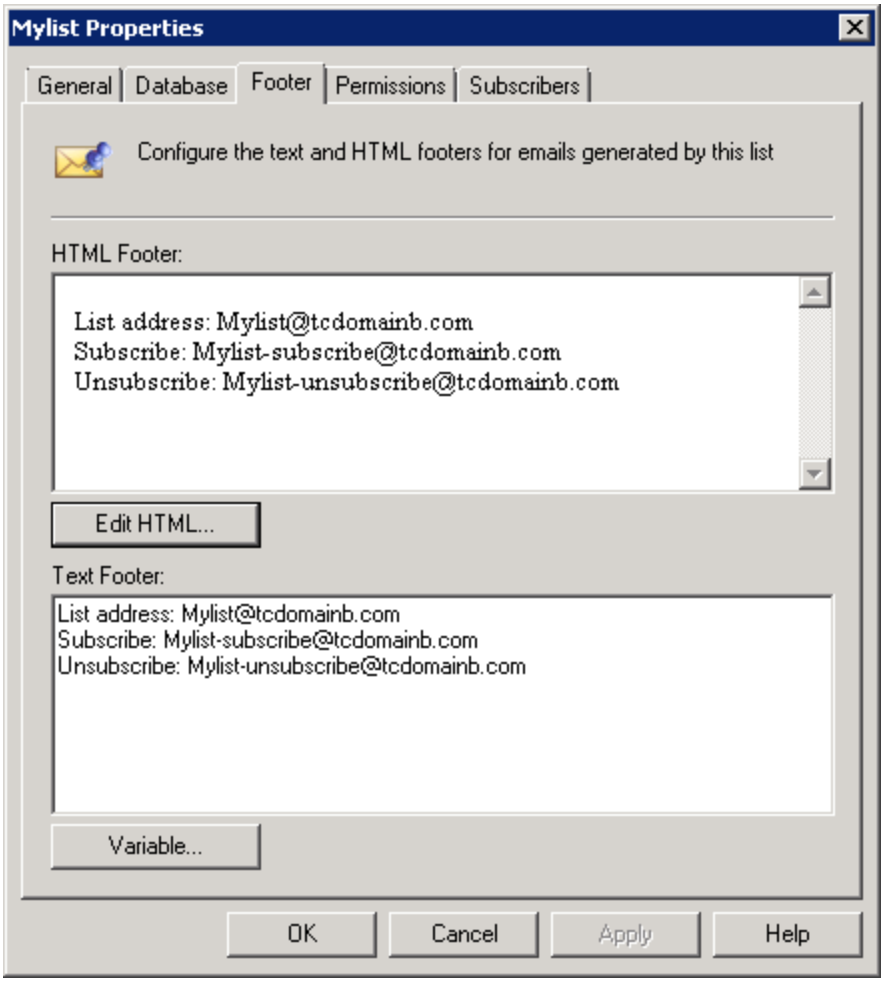
10.3.3 Configuring advanced newsletter/discussion list properties

After creating a new list, further options can be configured which enable the customization of elements and behavior of the list. These options include:

- Creating a custom footer for the list
- Setting permissions to the list
- Securing newsletters with a password
- Manually adding subscribers to the list
- Importing subscribers to the list/database structure

Creating a custom footer for the list

Configure a custom HTML or text footer. A footer is added to each email sent to the list.



Screenshot 118: List footer properties

1. Right click the list to add a footer to and select **Properties**.
2. From **Footer** tab, click **Edit HTML** to create an HTML footer.

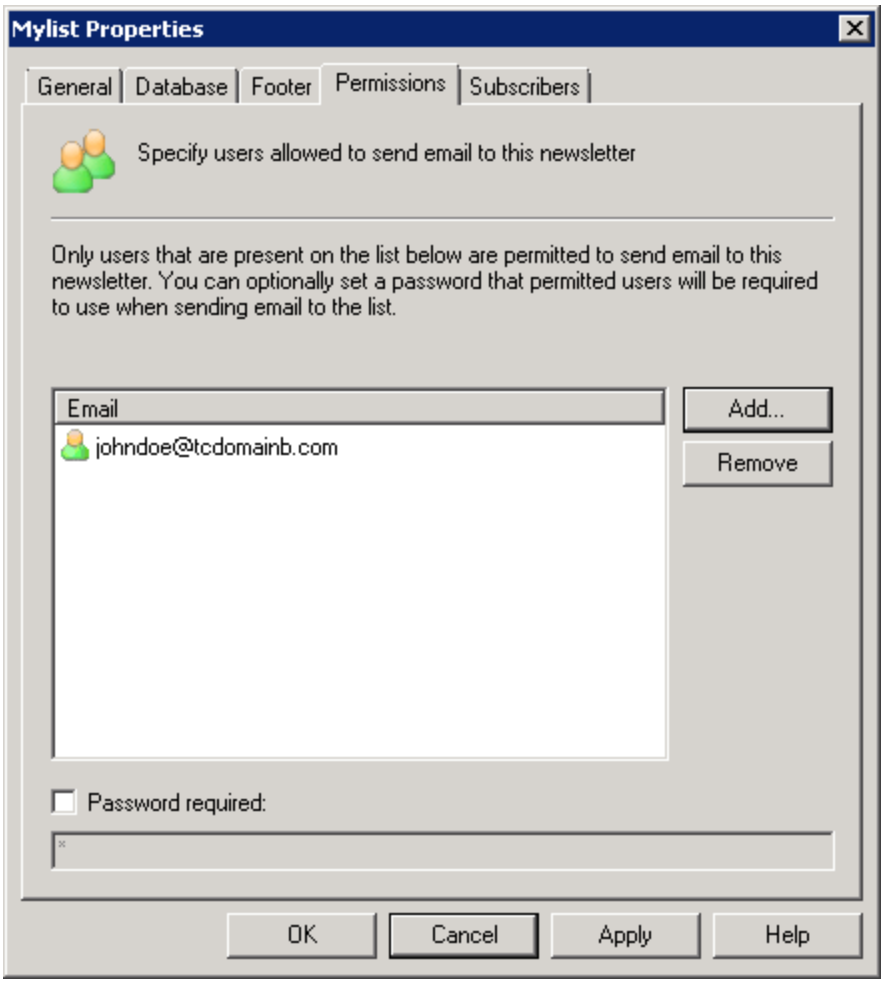
> **Tip**
>
> Use footers to show how users can subscribe and unsubscribe from list.

Setting permissions to the list

Specify who can submit an email to the list. If list is not secured, anyone can send emails to the entire list by sending an email to the list address.

> **NOTE**
>
> Permissions are not configurable for discussion lists.

1. Right click the list to set permissions for, and select **Properties**.



Screenshot 119: Setting permissions to the newsletter

2. From **Permissions** tab, click **Add**. Specify the users with permissions to submit an email to the list. Email addresses are added to **Email** list.

3. Enable passwords by selecting the **Password required:** checkbox and providing a password. For more information how to use this feature refer to the Securing newsletter with a password section below.

Securing newsletters with a password

Set a password that secures access to newsletter in case someone else makes use of the email client or account details of a permitted user.

> **NOTE**
>
> Discussion lists cannot be secured with passwords.

1. Right click the list to set permissions for, and select **Properties**.
2. From **Permissions** tab, select **Password required:** checkbox and provide a password.

> **IMPORTANT**
>
> When sending emails to the newsletter, users must authenticate themselves by including the password in the email subject field. Password must be specified in the subject field as follows:
>
> `[PASSWORD:<password>] <Subject of the email>`
>
> **Example:** `[PASSWORD:letmepost]Special Offer.`

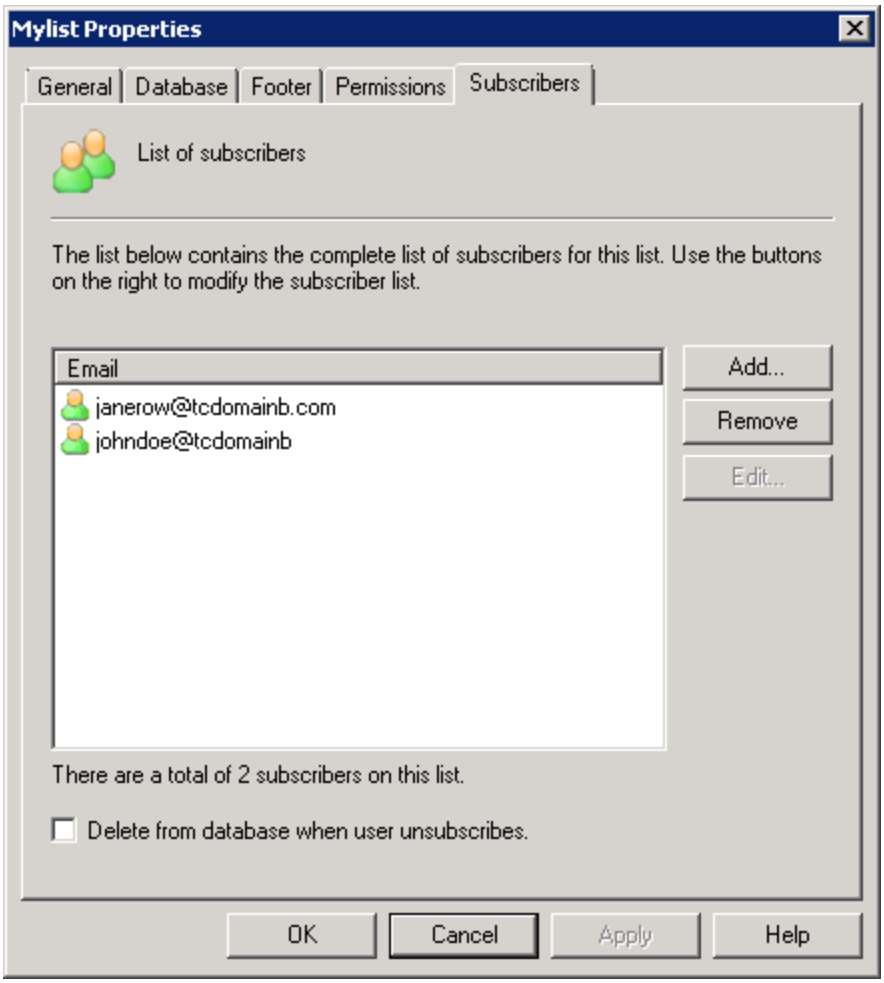
If password is correct, list server removes the password details from subject and relays email to Newsletter.

Manually adding subscribers to the list

Manually add users to newsletters/discussions without any action on their behalf.

> **NOTE**
>
> It is highly recommended that users subscribe themselves to the list by sending an email to the subscribe newsletter/discussion address.Ensure that you have the users' authorization before manually adding the users to the list.

1. Right click the list to set permissions for, and select **Properties**.



Screenshot 120: Entering subscribers to the newsletter

2. From **Subscribers** tab, click **Add**.
3. Key in 'Email Address', 'First name', 'Last name' and 'Company fields' and click **OK**. The new subscriber email address is added to **Email** list.

NOTE

First name, last name and company fields are optional.

NOTE

To remove subscribers from list, select user and click **Remove** .

NOTE

To remove users from the subscription list table when unsubscribing from the list (and not just flag them as unsubscribed) select **Delete from database when user unsubscribes** checkbox.

Importing subscribers to the list / database structure

When a new newsletter or discussion list is created, a table called 'listname_subscribers' with the following fields as shown in the table below is created.

To import data into the list, populate the database with data in the following fields.

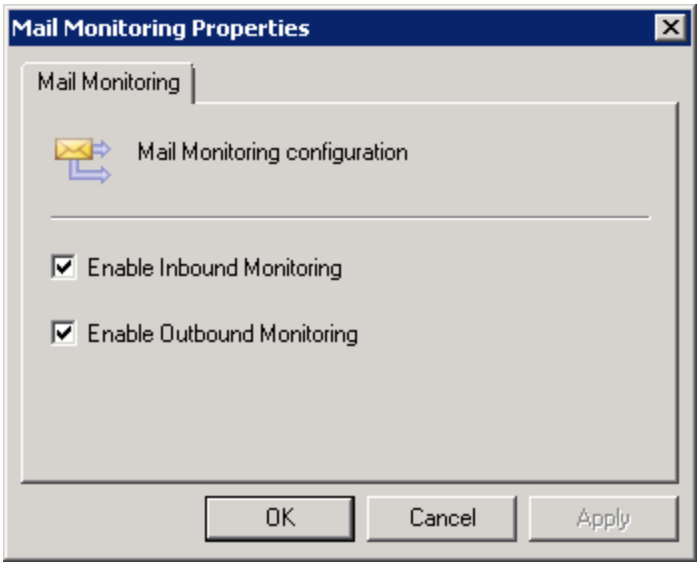
Field Name	Type	Default Value	Flags	Description
Ls_id	Varchar(100)		PK	Subscriber ID
Ls_first	Varchar(250)			First name
Ls_last	Varchar(250)			Last name
Ls_email	Varchar(250)			Email
Ls_unsubscribed	Int	0	NOT NULL	Unsubscribe flag
Ls_company	Varchar(250)			Company name

10.4 Mail Monitoring

Mail monitoring enables copying emails sent to or from a particular local email address to another email address. This enables the creation of central store of email communications for particular persons or departments.

10.4.1 Enabling/Disabling email monitoring

1. Click **Start > All Programs > GFI MailEssentials > Email Management Tools** to load Email Management Tools.
2. Right click **Email management > Mail Monitoring** and select **Properties**.



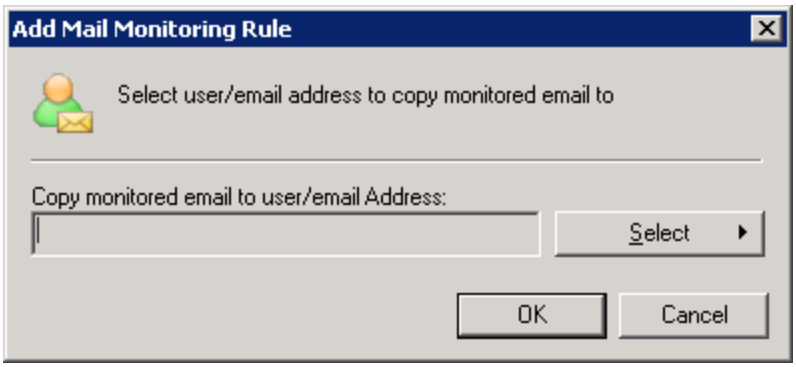
Screenshot 121: Enable or disable email monitoring

3. Enable/disable all inbound and outbound email monitoring rules by checking/unchecking **Enable Inbound Monitoring** and **Enable Outbound Monitoring** checkboxes.
4. Click **OK** to save changes.

> **NOTE**
>
> Enable/disable individual email monitoring rules by right click on the email monitoring rule and selecting **Enable/Disable**.

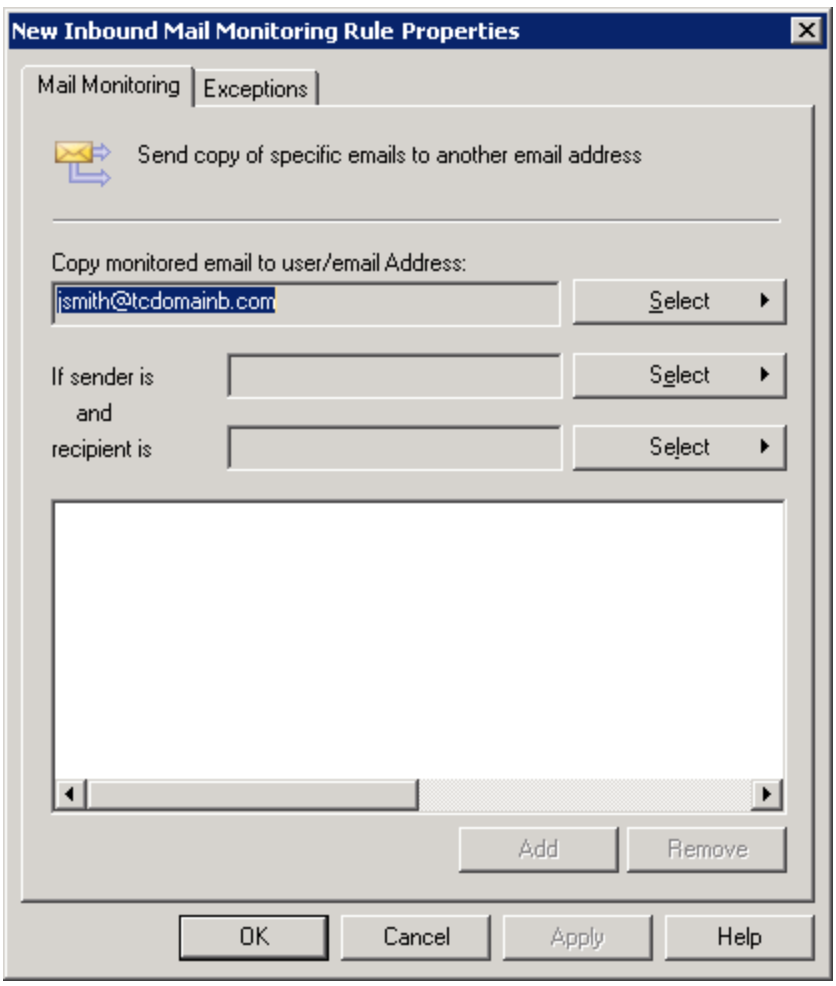
10.4.2 Configure email monitoring

1. Right click **Email management > Mail Monitoring** node and select **New > Inbound Mail Monitoring Rule** or **Outbound Mail Monitoring Rule** to monitor inbound or outbound email respectively.



Screenshot 122: Add Mail Monitoring rule

2. Key in the destination email address/mailbox to copy the emails to. Click **OK** to continue.



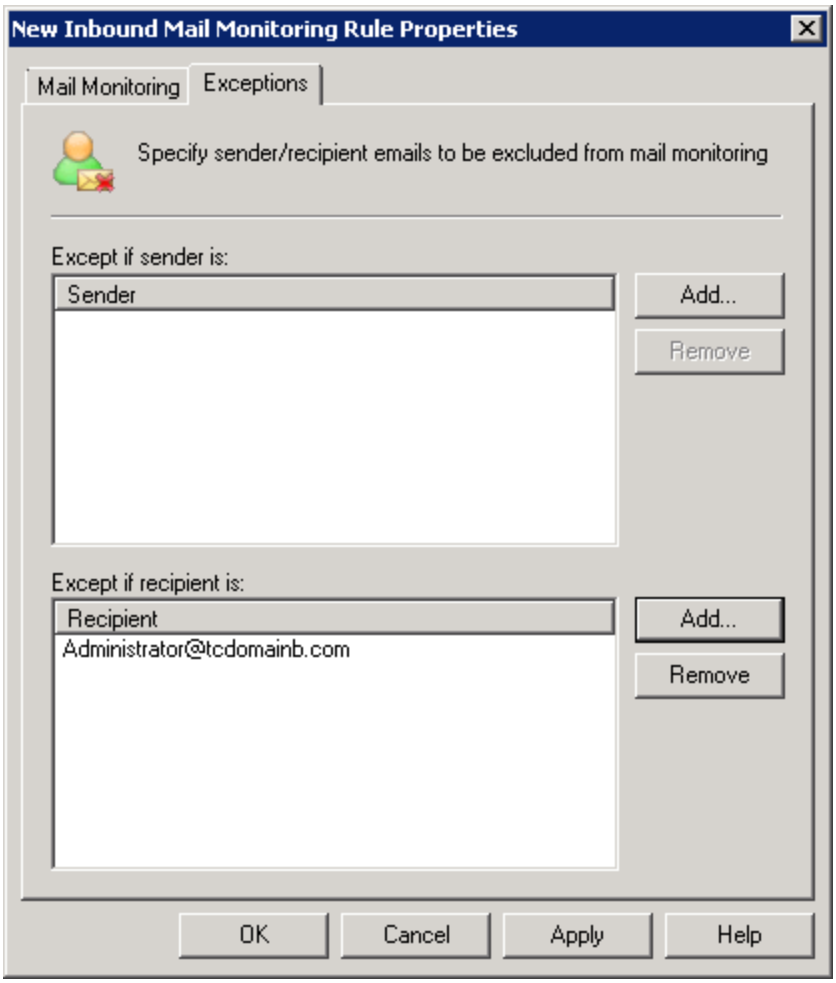
Screenshot 123: Configuring email monitoring

3. Click sender and recipient Select buttons to specify which emails this rule should monitor. Click **Add** to add filters to the list. Repeat to specify multiple filters. The following conditions can be monitored:

NOTE

To monitor all mail, key in: `*@*`

Condition	Rule
All email sent by a particular user	Create outbound rule, specify sender email or select user (if using AD) in the sender field and key in *@* as the recipient's domain.
All email sent to a particular user	Create inbound rule, specify recipient email or select user (if using AD) in the recipient field and specify *@* as the sender's domain.
Mail sent by a particular user to an external recipient	Create an outbound rule, specify sender or select user (if using AD) in the sender field. Key in external recipient email in the recipient field.
Mail sent to a particular user by an external sender	Create an inbound rule and specify external sender email in the sender field. Key in the username or user email address in the recipient field.
Mail sent by a particular user to a company or domain	Create an outbound rule and specify sender or select user (if using AD) in the sender field. Specify the domain of the company in the recipient field by selecting the domain via the recipient button.
Mail sent to a particular user by a company or domain	Create an inbound rule and specify domain of the company in the sender field. Select domain when clicking on the sender button and enter username or user email address in the recipient field.



Screenshot 124: Creating an exception

4. Select the Exceptions tab to add senders or recipients who will be excluded from the new rule. The available options are:

Option	Description
Except if sender is	Excludes the specified sender from the list.
Except if recipient is	Excludes the specified recipient from the list.

> **NOTE**
>
> When specifying exceptions for inbound monitoring rules, the Sender list contains non-local email addresses and the Recipient list addresses are all local. When specifying exceptions for an outbound monitoring rule, the Sender list contains local email addresses, whilst the Recipient list contains only non-local email addresses.

> **NOTE**
>
> Both exception lists apply and all senders listed in the sender exception list and all recipients listed in the recipient list will not be monitored.

5. Click **OK** to finalize settings.

> **NOTE**
>
> The new email monitoring rule can be renamed by clicking on the rule and pressing the F2 key.

11 General Settings

Topics in this chapter:

11.1 Administrator email address 219

11.2 Enabling/Disabling scanning modules 219

11.3 Proxy settings 221

11.4 Local domains 222

11.5 Managing local users 222

11.6 SMTP Virtual Server bindings 223

11.7 Version information 224

11.8 Patch Checking 225

11.9 Access Control 225

11.1 Administrator email address

GFI MailEssentials sends important notifications to the administrator via email. To set up the administrator's email address:

1. From the GFI MailEssentials Configuration navigate to **General Settings > Settings** and select the **General** tab.

Administrator email
Enter the administrator's email address in the field below. Notifications sent to the administrator will be sent to this email address.
Administrator Email:
Administrator@mydomain.com
NOTE: GFI MailEssentials will communicate this email address to the GFI servers. GFI will only use this email address to send important GFI MailEssentials notices directly to the administrator.

Screenshot 125: Specifying the administrator's email address

2. Key in the administrator's email address in the **Administrator email** area.

3. Click **Apply**.

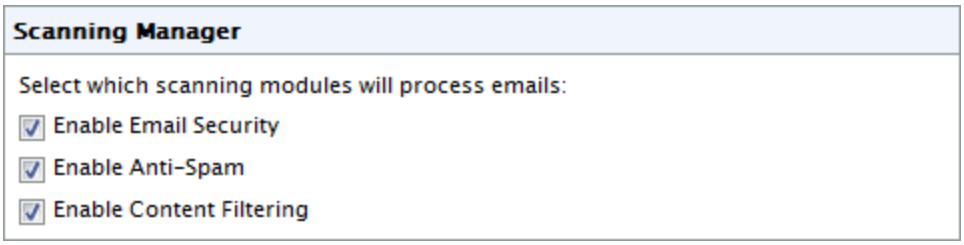
11.2 Enabling/Disabling scanning modules

From GFI MailEssentials you can enable or disable particular email scanning modules. This allows switching on and off scanning engines or filters in batch.

NOTE

This feature enables or disables particular scanning engines only. Disabled engines do not process inbound, outbound and/or internal emails. All other features of GFI MailEssentials, such as the quarantine store, is still functional.

1. From the GFI MailEssentials Configuration, navigate to **General Settings > Settings** and select the **General** tab.



Screenshot 126: Scanning Manager

2. Enable or disable scanning modules:

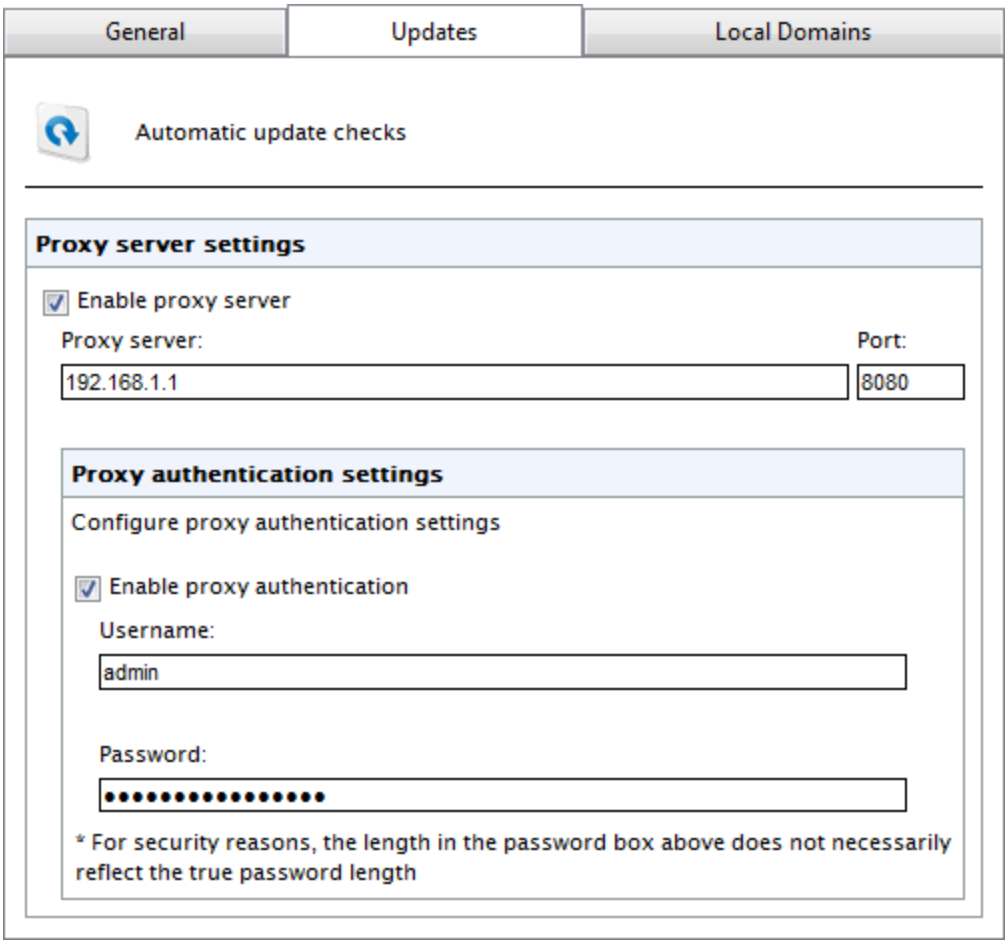
Option	Description
Enable Email Security	Enables/Disables the following scanning engines: » Virus Scanning Engines » Information Store Protection » Trojan & Executable Scanner » Email Exploit Engine » HTML Sanitizer
Enable Anti-Spam	Enables/Disables the following anti-spam filters: » SpamRazer » Anti-Phishing » Directory Harvesting » Email Blocklist » IP DNS Blocklist » URI DNS Blocklist » Greylist » Language Detection » Bayesian Analysis » Whitelist » New Senders
Enable Content Filtering	Enables/Disables the following content filtering engines: » Keyword Filtering » Attachment Filtering » Decompression Engine » Advanced Content Filtering

3. Click **Apply**.

11.3 Proxy settings

GFI MailEssentials automatically checks for and downloads updates (for example, virus definitions updates and SpamRazer definitions) from the Internet. If the server on which GFI MailEssentials is installed, connects to the Internet through a proxy server, configure the proxy server settings as follows:

1. From GFI MailEssentials Configuration go to **General Settings > Settings** and select **Updates** tab.



Screenshot 127: Updates server proxy settings

2. Select the **Enable proxy server** checkbox.

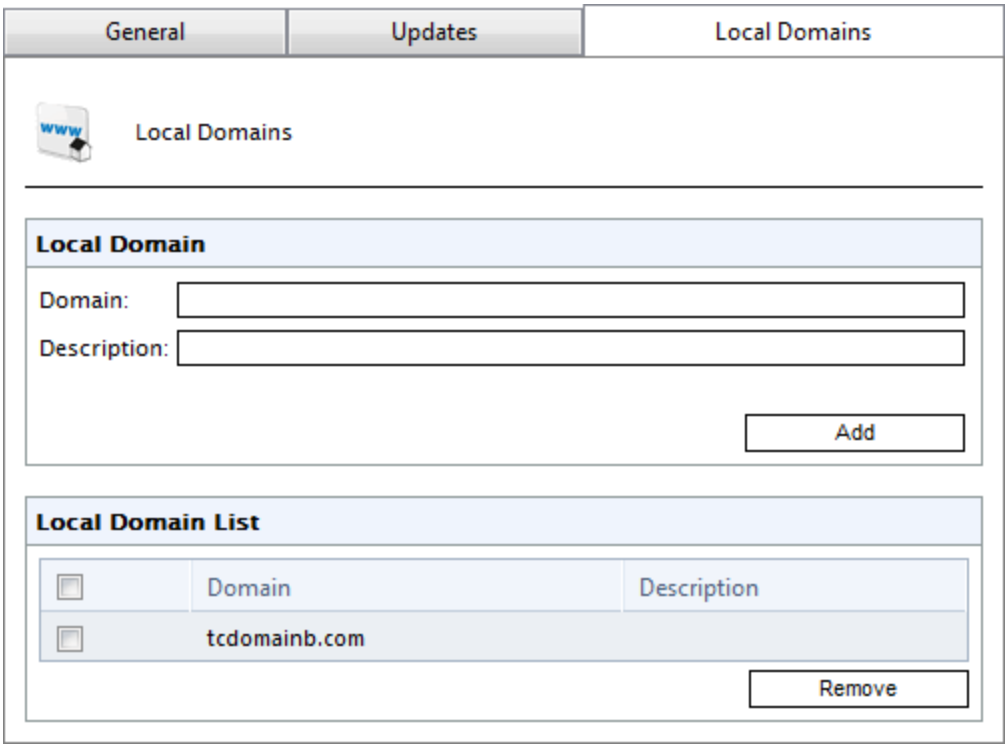
3. In the **Proxy server** field key in the name or IP address of the proxy server.

4. In the **Port** field, key in the port to connect on (default value is 8080).

5. If the proxy server requires authentication, select **Enable proxy authentication** and key in the **Username** and **Password**.

6. Click **Apply**.

11.4 Local domains



Screenshot 128: Local Domains list

GFI MailEssentials requires the list of local domains to enable it to distinguish between inbound, outbound or internal emails. During installation or post install wizard, GFI MailEssentials automatically imports local domains from the IIS SMTP service or Microsoft® Exchange Server. In some cases, however, local domains may have to be added manually.

IMPORTANT

GFI MailEssentials only filter emails destined to local domains for spam. Some rules filter are also based on the direction. This is determined by the local domains

To add or remove local domains after installation, follow these steps:

1. Go to **General Settings > Settings** and select **Local Domains** tab.
2. Key in the name and description of the domain to add in the **Domain** and **Description** text boxes.
3. Click **Add** to include the stated domain in the **Local domains** list.

NOTE

To remove a listed domain, select it from the list and click **Remove**.

4. Click **Apply**.

11.5 Managing local users

GFI MailEssentials uses 3 ways to retrieve users depending on the installation environment.

> **NOTE**
>
> The number of users retrieved is also used for licensing purposes.

11.5.1 GFI MailEssentials installed in Active Directory mode

When GFI MailEssentials is not installed on the same machine as your mail server and Active Directory is present, then GFI MailEssentials retrieves mail-enabled users from the Active Directory domain of which the GFI MailEssentials machine forms part.

GFI MailEssentials installed on the Microsoft® Exchange machine

When GFI MailEssentials is installed on the same machine as Microsoft® Exchange, GFI MailEssentials retrieves the Active Directory users that have a mailbox on the same Microsoft® Exchange Server.

11.5.2 GFI MailEssentials installed in SMTP mode

When you choose to install GFI MailEssentials in SMTP mode, the list of local users is stored in a database managed by GFI MailEssentials.

To populate and manage the user list when GFI MailEssentials is installed in SMTP mode, go to **General > Settings** and select the **User Manager** tab.

The **User Manager** tab displays the list of local users and allows you to add or remove local users. The list of local users is used when configuring user-based rules, such as **Attachment Filtering** rules and **Content Filtering** rules.

> **NOTE**
>
> GFI MailEssentials automatically populates the list of local users using the sender's email address in outbound emails.

To add a new local user:

1. Enter the email address in the **Email address** box.
2. Click **Add**.
3. Repeat to add more local users and click **Apply**.

To remove a local user:

1. Select the local user you want to remove from the **Local Users** list and click **Remove**.
2. Repeat to remove more local users and click **Apply**.

11.6 SMTP Virtual Server bindings

GFI MailEssentials always binds to the first SMTP virtual server configured in IIS. In case of multiple SMTP virtual servers, GFI MailEssentials may be required to be bound to a new or a different SMTP Virtual Server.

NOTE

The SMTP Virtual Server Bindings tab is not displayed if you installed GFI MailEssentials on a Microsoft® Exchange Server 2007/2010 machine.

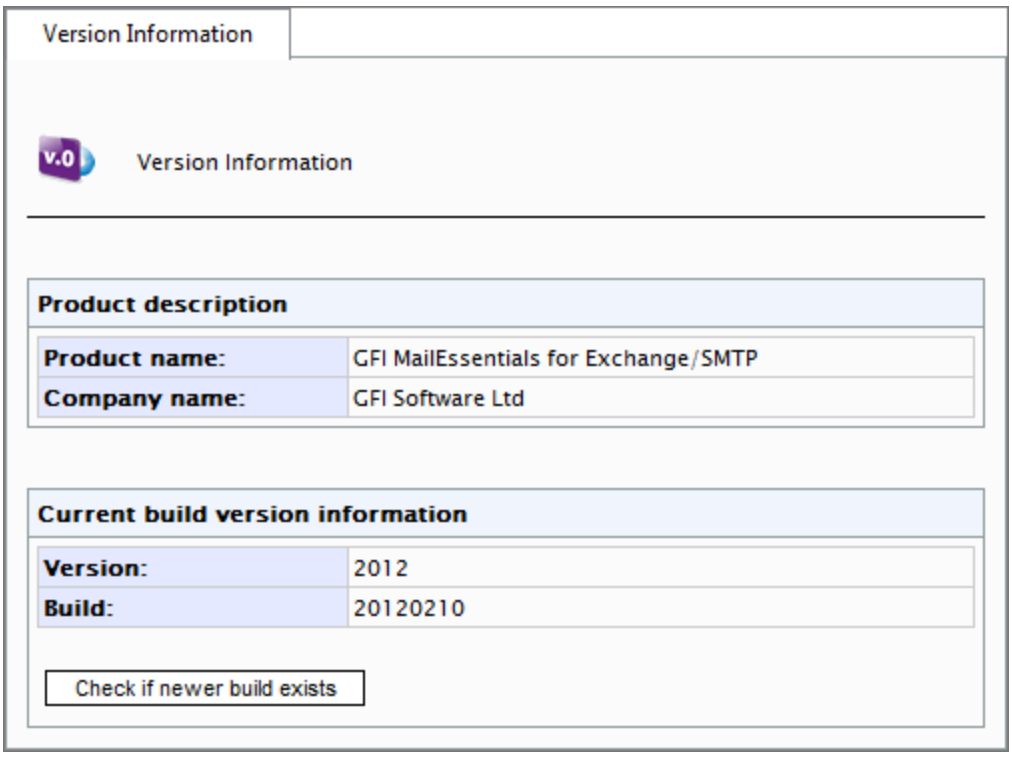
11.6.1 Binding GFI MailEssentials to another other SMTP Virtual Server.

NOTE

Some services are temporarily stopped while performing this operation. This may affect mail flow and/or email scanning.

1. Go to **General Settings > Settings** and click **Bindings** tab.
2. Select the SMTP Virtual Server to bind GFI MailEssentials to.
3. Click **Apply**.
4. GFI MailEssentials will ask to restart services for the new settings to take effect.

11.7 Version information



Screenshot 129: Version Information page

To view the GFI MailEssentials version information, navigate to **General Settings > Version Information**. The version information page displays the GFI MailEssentials installation version and build number.

To check whether you have the latest build of GFI MailEssentials installed on your machine, click **Check if newer build exists**.

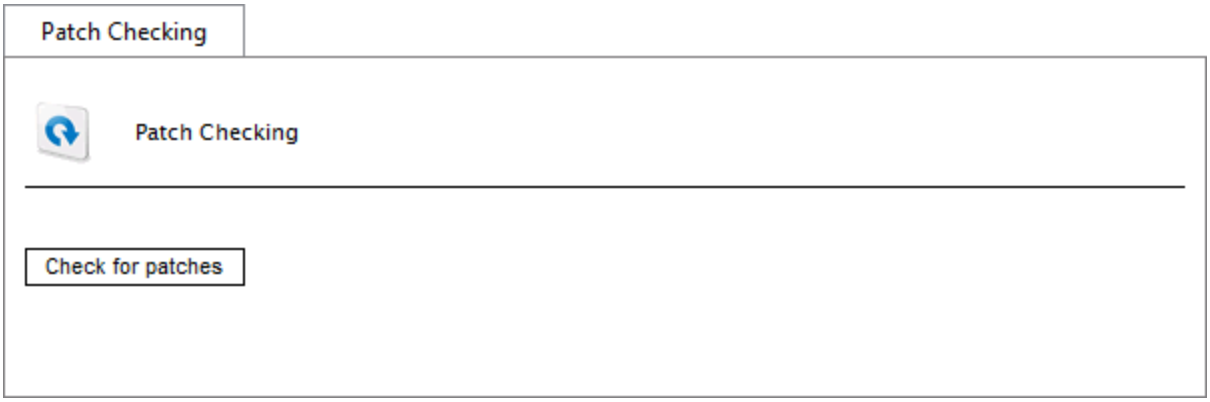
> **NOTE**
>
> Always quote your GFI version and build information when contacting GFI support.

11.8 Patch Checking

The Patch Checking feature verifies if there are any software patches available for your version of GFI MailEssentials by directly connecting to the GFI Update Servers.

> **NOTE**
>
> It is highly recommended to check for patches periodically to keep GFI MailEssentials updated.

1. Navigate to **General Settings > Product Patches**.



Screenshot 130: Checking for product patches

2. Click **Check for patches** to connect to the GFI Update Server and check for available updates.
3. Click the **Download** link of patches to download.
4. On completion, install the downloaded updates.

> **NOTE**
>
> To access the installation instructions and other information applicable to a patch, click the information link provided in the list of available updates. An incorrect patch installation might cause the product to malfunction or degrade its performance.

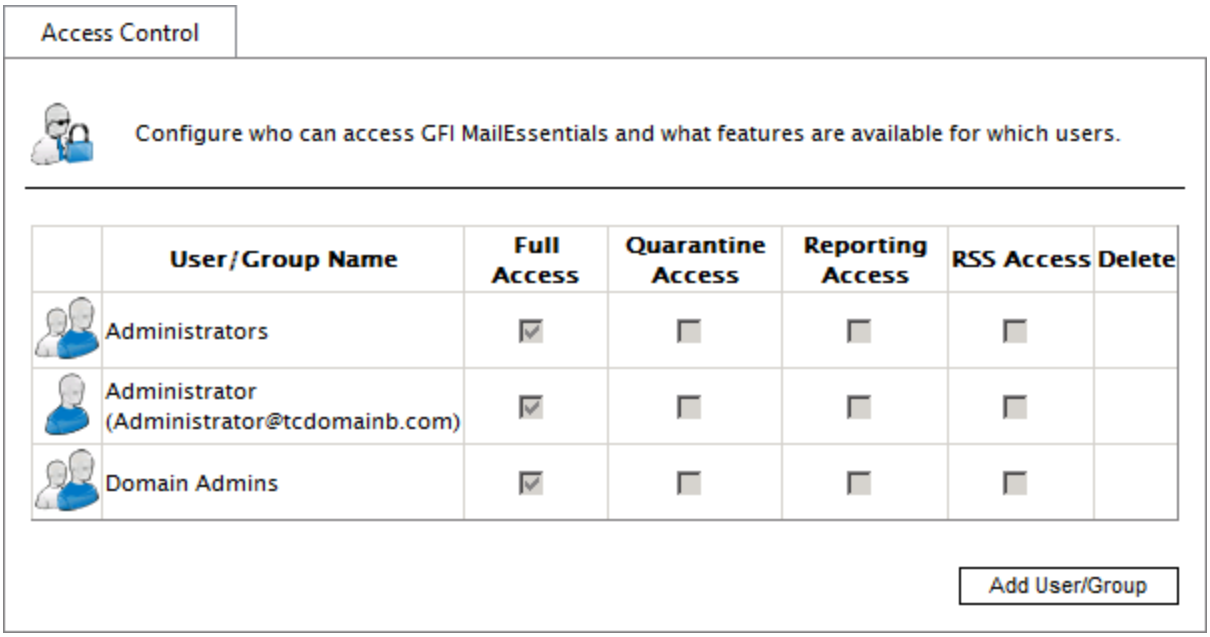
11.9 Access Control

Allow or block access to various features of GFI MailEssentials for particular domain users or groups. Users can access the Web UI of GFI MailEssentials using their domain credentials. The features shown to logged in users depends on the Access Control configuration.

NOTE

Configuring Web UI access is only possible when GFI MailEssentials is running in IIS mode and can be accessed over the network (including different trusted domains). Access Control is not configurable when GFI MailEssentials is running in Local mode. For more information, refer to User interface mode (page 227).

1. From GFI MailEssentials Configuration, go to **General Settings > Access Control**. Add domain users or groups and select the product features to allow access to.



Screenshot 131: Access control settings

2. Click **Add User/Group**.

3. In the **User Lookups** dialog, enter the name of the user or group to add and click **Check Names**.

4. GFI MailEssentials displays the list of users/groups found. Select the users/groups to add and click **Submit**.

5. For the newly added users/groups, select the features to allow access to.

Permission	Description
Full Access	User can access and configure all features of the product.
Quarantine Access	Allows access to quarantine search and search folders.
Reporting Access	Enables users to generate reports.
RSS Access	Allows users to subscribe to the quarantine RSS feeds.

6. Click **Apply**.

12 Miscellaneous topics

Topics in this chapter:

12.1 Virtual directory names 227

12.2 User interface mode 227

12.3 Failed emails 231

12.4 Tracing 233

12.5 POP2Exchange - Download emails from POP3 server 235

12.6 Moving spam email to user's mailbox folders 238

12.7 Move spam to Exchange 2010 folder 240

12.8 Synchronizing configuration data 241

12.9 Disabling email processing 252

12.10 Email backup before and after processing 253

12.11 Remoting ports 254

12.12 Monitoring Virus Scanning API 255

12.1 Virtual directory names

The default virtual directory names of GFI MailEssentials and Quarantine RSS are **MailEssentials** and **MailEssentialsRSS** respectively. Virtual directory names are customizable; however it is recommended that these are not changed.

> **NOTE**
>
> If GFI MailEssentials is configured to be accessed only from the local machine, the GFI MailEssentials Configuration virtual directory is not configurable.

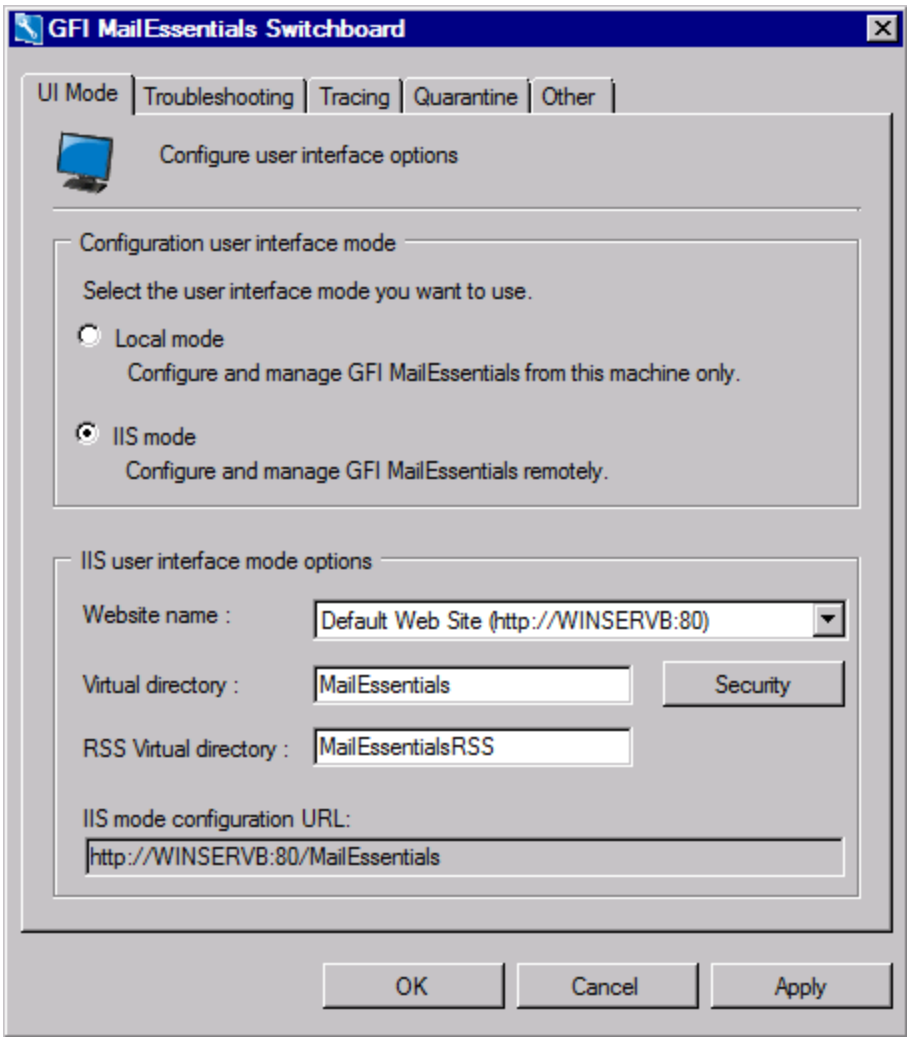
1. Launch GFI MailEssentials Switchboard from **Start > Programs > GFI MailEssentials > Switchboard**.
2. From **IIS user interface mode options** area, specify custom virtual directory names for:
   - GFI MailEssentials Configuration - key in a custom name in the **Virtual directory** field.
   - Quarantine RSS virtual directory - key in a custom name in the **RSS Virtual directory** field.
3. Click **Apply**.
4. Click **OK** and wait while applying the new settings.
5. When the process completes, click **OK**.

12.2 User interface mode

The GFI MailEssentials user interface can be loaded on the installation machine only (local mode) or accessible via http over the network (IIS mode).

To select the mode:

1. Launch the GFI MailEssentials Switchboard from **Start > Programs > GFI MailEssentials > Switchboard**.



Screenshot 132: GFI MailEssentials Switchboard - UI Mode

2. From the **UI mode** area, select:

Option	Description
Local mode	GFI MailEssentials loads in an html viewer application, accessible from the machine where GFI MailEssentials is installed only. **NOTE** If using Local mode: » Spam digest links will not work » User portal will not be available - users will not be able to manage personal whitelists and blocklists and their personal quarantine. For more information, refer to User Actions (page 62).
IIS mode (recommended)	GFI MailEssentials loads in your default web browser using the IIS setup settings configured during installation. User interface is also accessible over the network via http. **NOTE** IIS setup settings can be altered using the Website name, Virtual directory and RSS virtual Directory fields. The **Security** options enable the configuration of an Access Control List and the IIS Authentication.

NOTE

Some services are temporarily stopped while performing this operation. This may affect mail flow and/or email scanning.

3. Click **Yes** to restart the displayed services.
4. Click **OK**.

12.2.1 IIS Security Settings

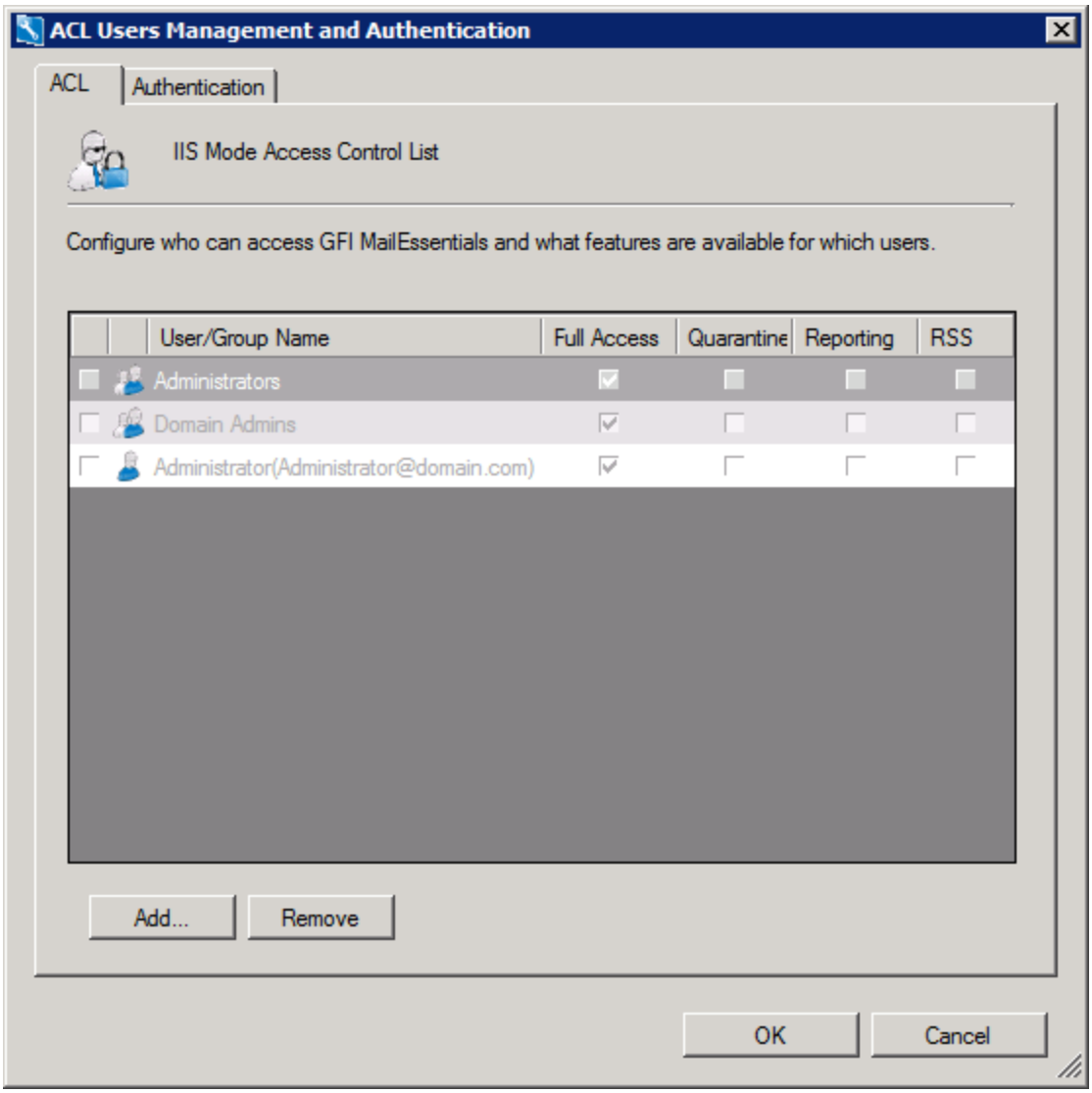
The **Security** button within the UI mode tab enables you to configure an Access Control List and Authentication method.

Access Control List

The Access control list specifies who can access GFI MailEssentials and what features are available for which users or groups. By default, Administrators are granted full access to GFI MailEssentials; you can however specify specific users or groups with different access types.

To add a user:

1. Load Switchboard by clicking **Start > Programs > GFI MailEssentials > Switchboard**.
2. Select **UI Mode** tab. Click **IIS Mode** and select **Security**.



Screenshot 133: IIS Security - ACL tab

3. Click **Add...** and provide the name of the user or group to add to the list.
4. Select the type of access to grant. Available options are:

- Full
- Quarantine
- Reporting
- RSS

5. Click **OK** to finalize setup.

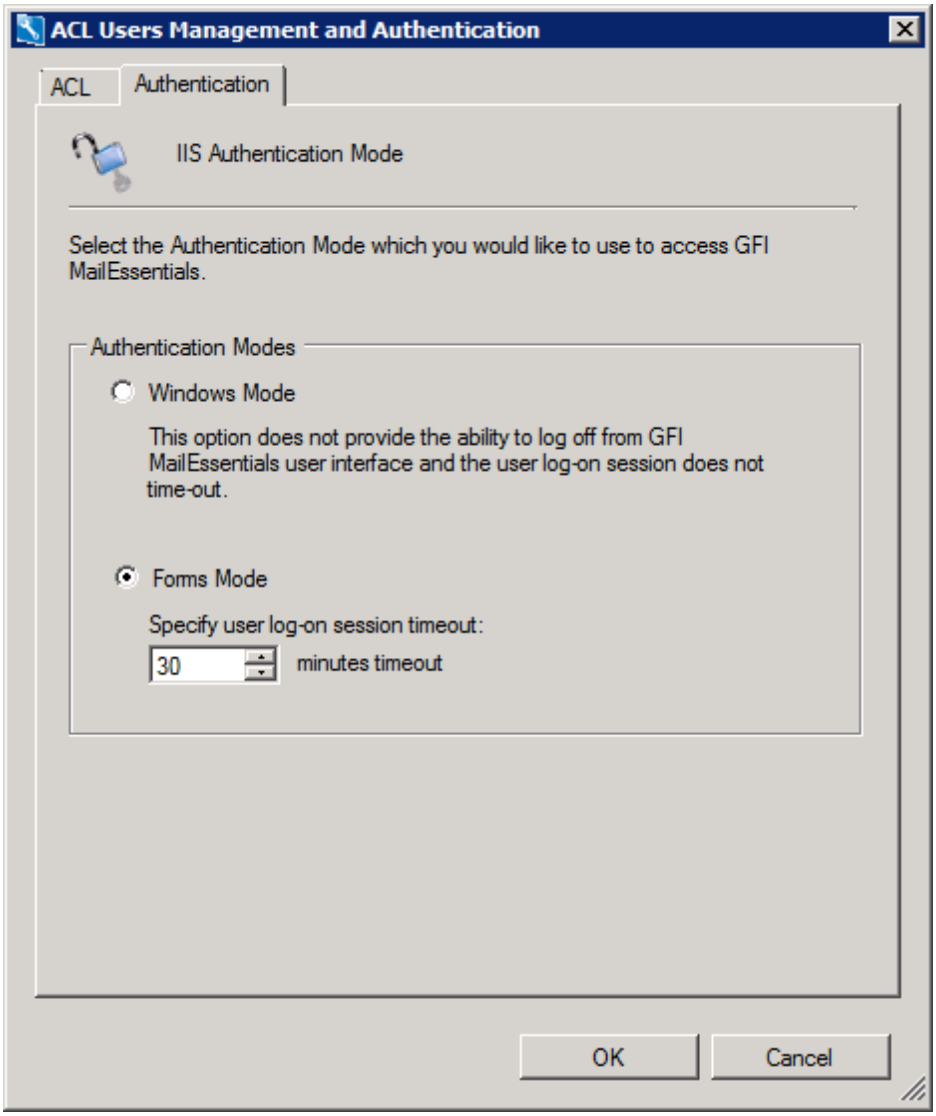
To remove access to a user or group, select the item to remove and click **Remove**.

IIS Authentication Mode

The IIS Authentication Mode enables you to choose the authentication method to use when accessing GFI MailEssentials.

1. Load Switchboard by clicking **Start > Programs > GFI MailEssentials > Switchboard**.
2. Select **UI Mode** tab. Click **IIS Mode** and select **Security**.

3. Select **Authentication** tab.


ACL Users Management and Authentication
ACL
Authentication
IIS Authentication Mode
Select the Authentication Mode which you would like to use to access GFI MailEssentials.
Authentication Modes
Windows Mode
This option does not provide the ability to log off from GFI MailEssentials user interface and the user log-on session does not time-out.
Forms Mode
Specify user log-on session timeout:
30
minutes timeout
OK
Cancel

Screenshot 134: IIS Security - Authentication tab

4. Select one of the available options:

Option	Description
Windows Mode	Windows authentication enables GFI MailEssentials to make use of the credentials of the currently logged on user and does not provide log-off and automatic timeout of the user interface session.
Forms Mode	(Default) Forms authentication provides the ability for users to log off. It also enables you to configure an automatic timeout from the user interface session. This is recommended if end users are accessing their GFI MailEssentials user console, especially if used from public computers.

5. Click **OK** to save settings.

12.3 Failed emails

There may be instances where the GFI MailEssentials email security or content filters cannot scan an email, for example, emails containing corrupted header information. In this case, GFI MailEssentials blocks the email since it may contain malicious content, and moves it to the following folder:

<GFI MailEssentials installation path>\EmailSecurity\failedmails

12.3.1 Reprocessing legitimate emails that fail

It is recommended to contact GFI Support when a number of emails are being moved to the **failedmails** folder. When the issue is resolved, emails can be re-scanned by GFI MailEssentials to determine if they are safe to be delivered.

> **NOTE**
>
> Files with extension .PROP in the **failedmails** folder are used for troubleshooting purposes. When reprocessing failed emails, these files can be deleted.

GFI MailEssentials installed on Microsoft® Exchange Server 2007/2010

1. In the **failedmails** folder, change the extension of .TXT files to .EML.

> **NOTE**
>
> To automatically change the extension of all .TXT files in the **failedmails** folder to .EML files, from command prompt change the directory to the **failedmails** folder and run the following command:
>
> `ren *.txt *.eml`

2. Move renamed files to the following folder:

<drive>\Program Files\Microsoft\Exchange Server\TransportRoles\Replay

GFI MailEssentials installed on Microsoft® Exchange Server 2003

Move emails (in .txt format) from the **failedmails** folder to the following folder:

<Microsoft Exchange installation path>\Exchsrvr\Mailroot\vsi 1\PickUp

GFI MailEssentials installed on Gateway server

Move emails (in .txt format) from the **failedmails** folder to the following folder:

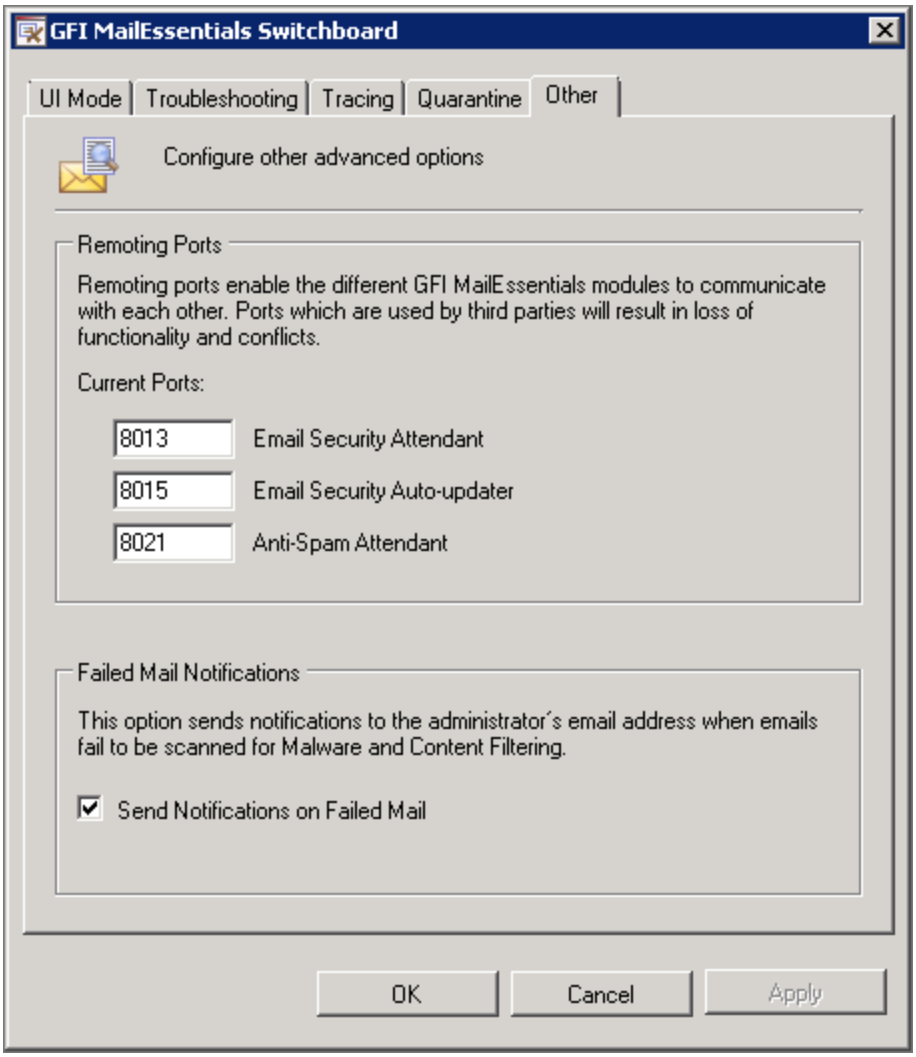
<drive>\Inetpub\mailroot\Pickup

12.3.2 Failed emails notifications

GFI MailEssentials can be configured to notify the administrator when an email fails processing.

The administrator's email address can be configured from GFI MailEssentials General Settings node. For more information, refer to Administrator email address (page 219).

1. Launch the GFI MailEssentials Switchboard from **Start > Programs > GFI MailEssentials > Switchboard** and select **Other** tab.


GFI MailEssentials Switchboard
UI Mode
Troubleshooting
Tracing
Quarantine
Other
Configure other advanced options
Remoting Ports
Remoting ports enable the different GFI MailEssentials modules to communicate with each other. Ports which are used by third parties will result in loss of functionality and conflicts.
Current Ports:
8013
Email Security Attendant
8015
Email Security Auto-updater
8021
Anti-Spam Attendant
Failed Mail Notifications
This option sends notifications to the administrator's email address when emails fail to be scanned for Malware and Content Filtering.
Send Notifications on Failed Mail
OK
Cancel
Apply

Screenshot 135: Enabling Failed emails notification

2. Select **Send Notifications on Failed Mail**.

3. Click **Apply**.

> **NOTE**
>
> Some services are temporarily stopped while performing this operation. This may affect mail flow and/or email scanning.

4. Click **Yes** to restart the displayed services.

5. Click **OK**.

12.4 Tracing

GFI MailEssentials provides the facility of creating log files for debugging purposes. Use tracing for troubleshooting purposes or when contacting GFI Support. Disable tracing if there are performance issues with the GFI MailEssentials machine.

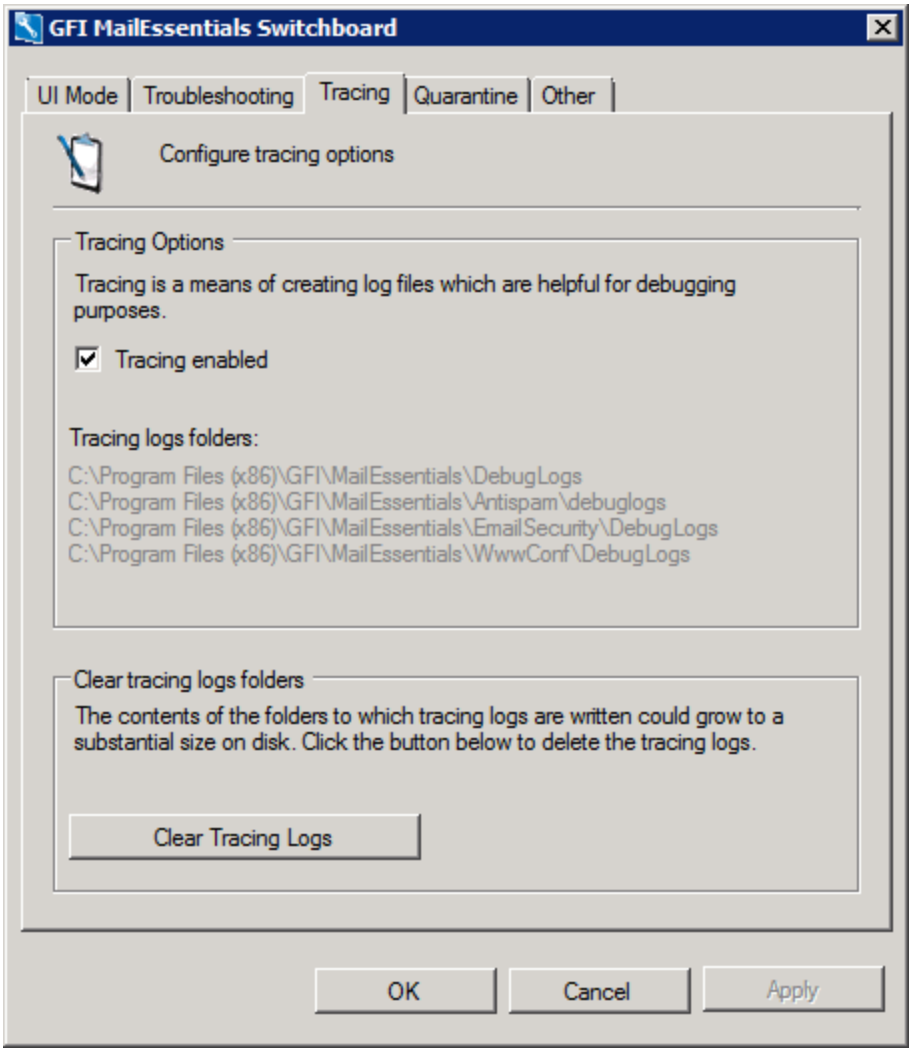
When enabled, GFI MailEssentials stores a number of log files in the following folders:

- <*GFI MailEssentials installation path*>*GFI**MailEssentials*\DebugLogs\
- <*GFI MailEssentials installation path*>*GFI**MailEssentials*\DebugLogs\

- <*GFI MailEssentials installation path*>*GFI**MailEssentials*\AntiSpam\DebugLogs\
- <*GFI MailEssentials installation path*>*GFI**MailEssentials*\WwwConf\DebugLogs\

To enable or disable Tracing:

1. Launch the GFI MailEssentials Switchboard from **Start > Programs > GFI MailEssentials > Switchboard** and select **Tracing** tab.


GFI MailEssentials Switchboard
UI Mode
Troubleshooting
Tracing
Quarantine
Other
Configure tracing options
Tracing Options
Tracing is a means of creating log files which are helpful for debugging purposes.
Tracing enabled
Tracing logs folders:
C:\Program Files (x86)\GFI\MailEssentials\DebugLogs
C:\Program Files (x86)\GFI\MailEssentials\Antispam\debuglogs
C:\Program Files (x86)\GFI\MailEssentials\EmailSecurity\DebugLogs
C:\Program Files (x86)\GFI\MailEssentials\WwwConf\DebugLogs
Clear tracing logs folders
The contents of the folders to which tracing logs are written could grow to a substantial size on disk. Click the button below to delete the tracing logs.
Clear Tracing Logs
OK
Cancel
Apply

Screenshot 136: Configuring Tracing options

2. Select or unselect **Tracing enabled** to enable or disable logging respectively.

> **NOTE**
>
> Some services are temporarily stopped while performing this operation. This may affect mail flow and/or email scanning.

3. Click **Yes** to restart the displayed services.

4. Click **OK**.

Clear Tracing Logs

To delete all Tracing logs:

1. Launch the GFI MailEssentials Switchboard from **Start > Programs > GFI MailEssentials > Switchboard** and select **Tracing** tab.

> **NOTE**
>
> Some services are temporarily stopped while performing this operation. This may affect mail flow and/or email scanning.

2. Click **Clear Tracing Logs** and click **Yes** to restart the displayed services.

3. Click **OK** when completed.

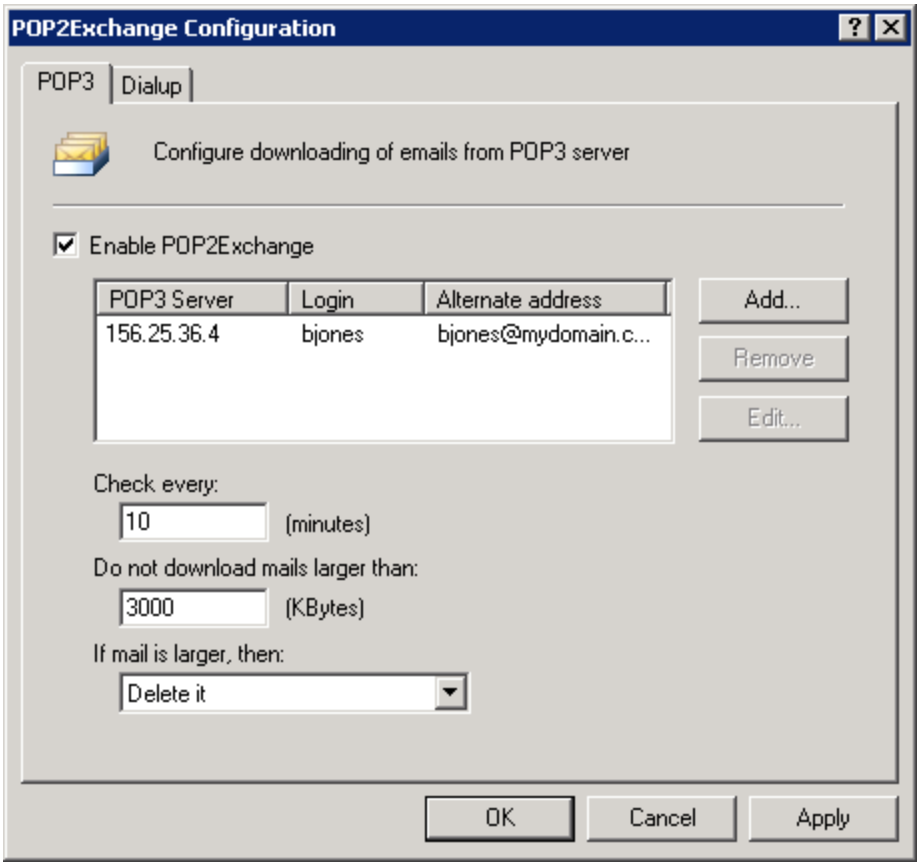
12.5 POP2Exchange - Download emails from POP3 server

POP2Exchange downloads emails from a POP3 server, processes them and sends them to the local mail server. The recommendation for GFI MailEssentials is to, if possible, avoid using POP3 and to use SMTP since POP3 is designed for email clients and not for mail servers. Notwithstanding this fact, and to cater for situations where a static IP address required by SMTP is not available, GFI MailEssentials can use POP3 to retrieve email.

12.5.1 Configuring POP3 downloader

1. From the GFI MailEssentials server, go to **Start > Programs > GFI MailEssentials > Email Management Tools**.

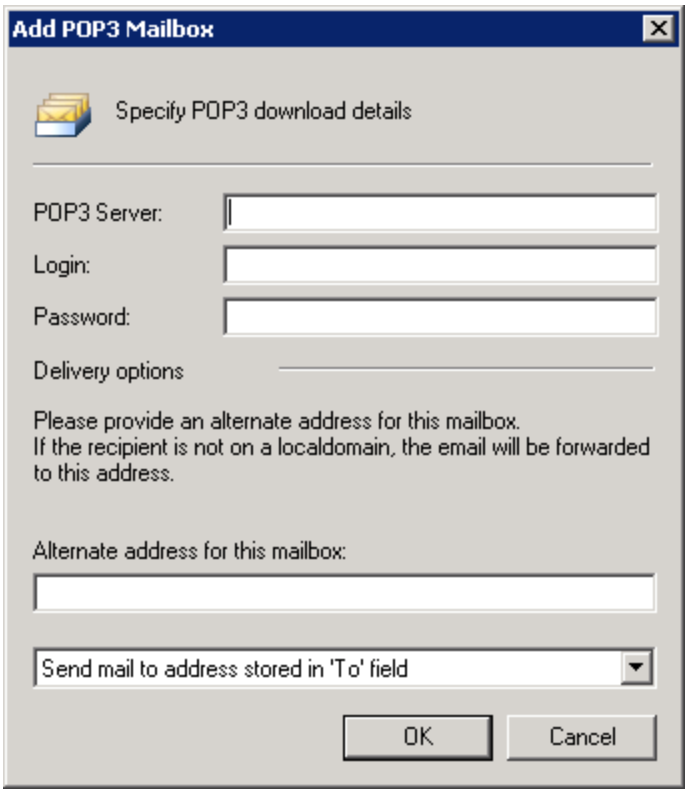
2. Select **POP2Exchange** node and double click **General**.



Screenshot 137: The GFI MailEssentials POP3 downloader

3. In the **POP3** tab, select **Enable POP2Exchange** to enable POP3 downloader.

4. Click **Add** to add a POP3 mailbox from which to download email.


Add POP3 Mailbox
Specify POP3 download details
POP3 Server:
Login:
Password:
Delivery options
Please provide an alternate address for this mailbox.
If the recipient is not on a localdomain, the email will be forwarded to this address.
Alternate address for this mailbox:
Send mail to address stored in 'To' field
OK
Cancel

Screenshot 138: Adding a POP3 mailbox

5. Key in the POP3 server details, mailbox login name and password of the mailbox. Choose between:

Option	Description
Send mail to address stored in 'To' field	GFI MailEssentials will analyze the email header and route the email accordingly. If email analyzing fails, email is sent to the email address specified in the alternate address field.
Send mail to alternate address	All email from this mailbox is forwarded to one email address. Enter full SMTP address in the **Email address** field.

6. Provide the alternate address and click **OK**.

NOTE

When specifying the destination email address (the address where GFI MailEssentials will forward the email to), ensure that you have set up a corresponding SMTP address on your mail server.

NOTE

Multiple POP3 mailboxes can be configured.

7. In the POP2Exchange configuration dialog, configure:

Option	Description
Check every (minutes)	Specify the download interval.
Do not download mail larger than (Kbytes)	Specify a maximum download size. If email exceeds this size, it will not be downloaded.

Option	Description
If mail is larger, then:	Choose to delete email larger than the maximum allowed size, or send a message to the postmaster.

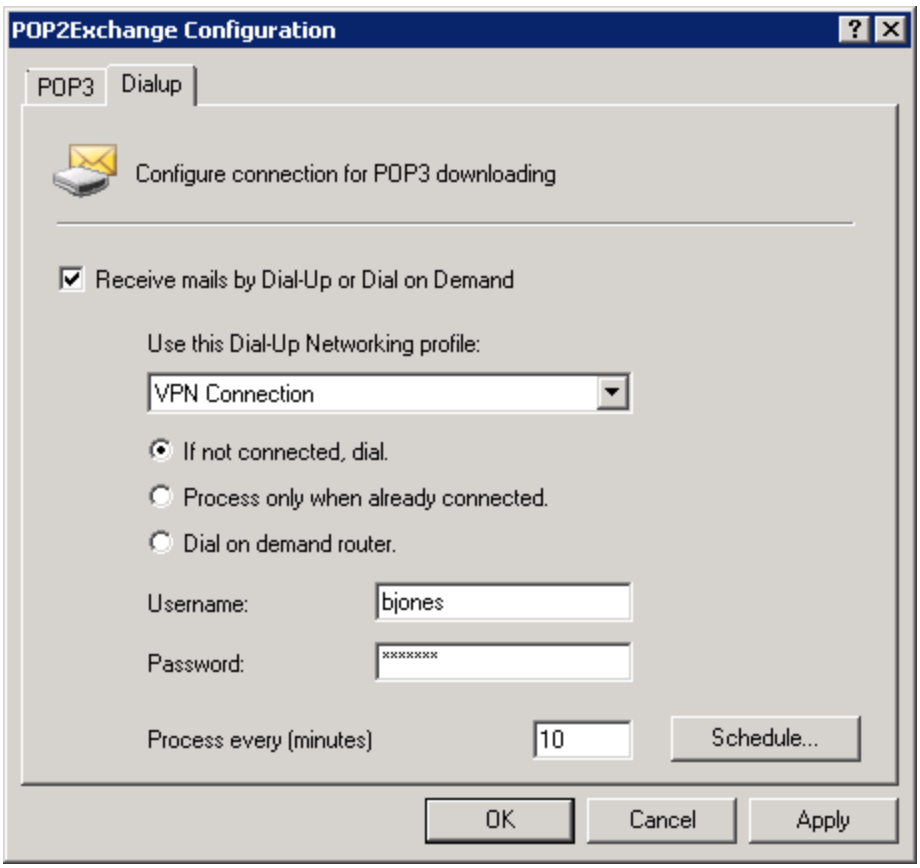
8. Click **OK**.

12.5.2 Configure dial up connection options

1. From the GFI MailEssentials server, go to **Start > Programs > GFI MailEssentials > Email Management Tools**.

2. Select **POP2Exchange** node and double click **General**.

3. From the **Dialup** tab select **Receive mails by Dial-Up or Dial on Demand**.

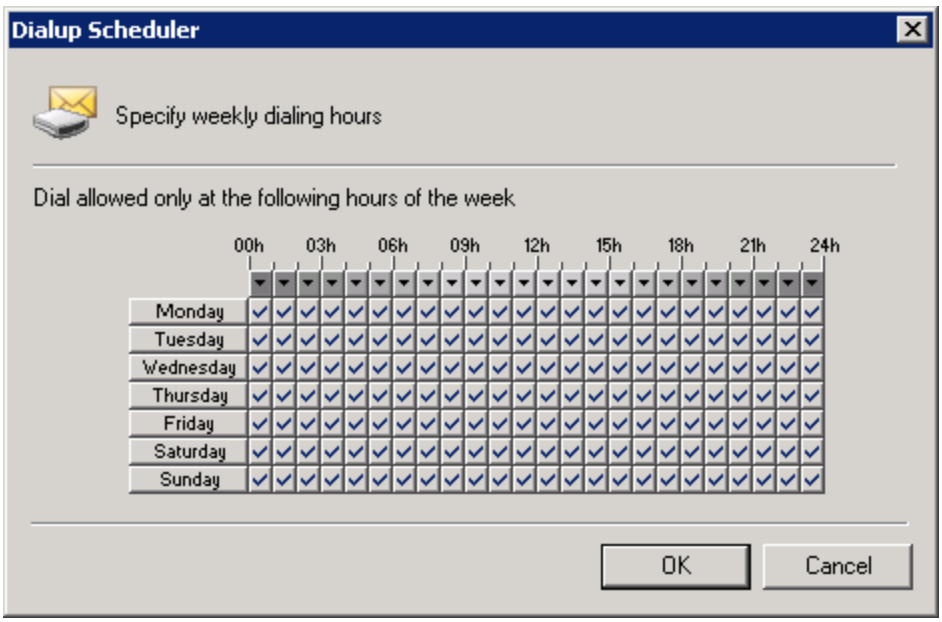


Screenshot 139: Dial-up options

4. Select a dial-up networking profile and configure a login name and password. The following options are available:

- **Use this Dial-Up Networking profile:** Choose the Dial-up Networking profile to use.
- **If not connected dial:**GFI MailEssentials will only dial-up if there is no connection.
- **Process only when already connected:**GFI MailEssentials will only process email if a connection already exists.
- **Dial on demand router:** In case of an Internet connection that is automatically established (such as a dial on demand router) select this option. GFI MailEssentials will pick up email at the specified interval without triggering a dial-up connection.
- **Username** & **Password**: Enter credentials used to logon to your ISP.

» **Process every (minutes):** Enter the interval at which GFI MailEssentials must connect to POP3 mailbox.



Screenshot 140: Configuring when to pick up email

5. Click **Schedule** and specify the hours when GFI MailEssentials should dial-up to pick up email. A check mark indicates that GFI MailEssentials will dial out. A cross indicates that GFI MailEssentials will not dial out at this hour.

6. Click **OK**.

12.6 Moving spam email to user's mailbox folders

When GFI MailEssentials is installed on the Microsoft® Exchange Server, spam emails can be saved in a user's mailbox folder. For more information, refer to Spam Actions - What to do with spam emails (page 135).

If GFI MailEssentials is **NOT** installed on the Microsoft® Exchange Server, spam emails cannot be routed to a specific user's mailbox folder through the Spam Actions. Emails can still however be routed to the user's mailbox as described below.

12.6.1 Microsoft® Exchange Server 2003

GFI MailEssentials includes a Rules Manager utility that automatically moves emails tagged as spam to the users' mailbox.

IMPORTANT

To use Rules Manager, in Spam Actions select the **Tag the email with specific text** option and specify a tag.

Install Rules Manager on the Microsoft® Exchange Server

1. From the GFI MailEssentials machine, go to:

<*GFI MailEssentials installation path*>\GFI\MailEssentials\Antispam\

2. Copy the following files to a folder on the Microsoft® Exchange Server:

- rulemgmtres.dll
- rulemgmt.exe
- rule.dll
- gfi_log.dll

3. From the Microsoft® Exchange Server, open command prompt and change the directory to the location where the Rules Manager files were copied.

4. In command prompt type: `regsvr32 rule.dll`

5. On confirmation, click **OK**.

Launch Rules Manager

1. From the Microsoft® Exchange Server, navigate to the location where Rules Manager files were copied and open **rulemgmt.exe**.

2. Select a Microsoft® Outlook profile (MAPI profile) or create a new profile to login (when using the Rules Manager the first time only).

3. Click **OK** to launch the Rules Manager.

4. The main window of the rules manager displays all the mailboxes enabled on the Microsoft® Exchange Server. The color of the mailboxes indicates the status of that mailbox:

- Blue - mailbox has rules configured
- Black - mailbox has no rules configured.

Setting new rules

1. Check the mailboxes to set a rule on and click **Configure…**.

> **NOTES**
>
> 1. New rules can be added to mailboxes which already contain rules.
> 2. Select multiple mailboxes to configure the same rule applicable to all mailboxes.

2. In the **Rule Condition** text box, type the tag given to the spam email in the GFI MailEssentials spam actions.

3. Specify the **Rule action**:

- Select **Delete** to delete an email which has a subject that contains the rule condition
- Select **Move to:** to move spam email to a folder in the mailbox. Key in the folder path where to save the spam email. If you specify Inbox\Spam, then a spam folder will be created in the Inbox folder. If you specify just Spam, then the folder will be created at the top level (same level as Inbox).

4. Click **Apply** to save the set rules.

Managing multiple rules

More than one rule can be set on the same mailbox.

Example: Delete emails tagged with `[Phishing]` and move emails tagged with `[SPAM]` to Inbox\Spam folder.

1. Double click on a mailbox to launch the Rules dialog.

2. A list of rules applicable to the selected mailbox is displayed.

   - Click **Add rule** to add a new rule
   - Select a rule and click **Edit rule** to change settings of the selected rule
   - Select a rule and click **Delete rule** to delete the selected rule.

3. Click **Apply** to save settings.

12.6.2 Microsoft® Exchange 2007/2010

To configure Microsoft® Exchange 2007/2010 to forward tagged emails to the user's Junk E-mail mailbox folder, a Transport Rule needs to be created.

> **IMPORTANT**
>
> In GFI MailEssentials Spam Actions select the Tag the email with specific text option only. If you select any other action, the emails detected as spam will not reach the mailbox of the user, and therefore the configured transport rules will not be applicable.

To create a Transport Rule in Exchange 2007/2010:

1. Launch the Microsoft® Exchange Management Console.

2. Navigate to **Microsoft Exchange > Organization Configuration > Hub Transport** and select the **Transport Rules** node.

3. Click **New Transport Rule**.

4. Type a name for the new rule (example, GFI MailEssentials `SPAM`) and click **Next**.

5. In the **Conditions** area, select **When the Subject field contains specific words**.

6. In the **Edit rule** area, click **Specific Words** to enter the words used for tagging. Type the tag specified in the spam actions of each spam filter (example, `[SPAM]`) and click **Add**. Click **OK** when all words are added and click **Next**.

7. In the **Actions** area, select **Set the spam confidence level to value**.

8. In the **Edit rule** area, click **0** and set the confidence level to **9**. Click **OK** and click **Next**.

9. (Optional) Set any exceptions to this transport rule and click **Next**.

10. Click **New** to create the new Transport Rule.

> **NOTE**
>
> Ensure that the Junk E-Mail folder is enabled for the users' mailboxes.

The transport rule created will now forward all emails which contain the GFI MailEssentials tag to the users' Junk E-mail folder.

12.7 Move spam to Exchange 2010 folder

When GFI MailEssentials is installed on a Microsoft® Exchange 2010 server, a dedicated user must be created for using the **Deliver email to mailbox - In Exchange mailbox sub-folder** anti-spam action.

Configure the dedicated user from the GFI MailEssentials Switchboard.

> **NOTE**
>
> If a user is not configured, spam cannot be moved to a mailbox sub-folder.

To configure a dedicated user:

1. Launch GFI MailEssentials Switchboard from **Start > Programs > GFI MailEssentials > Switchboard**.
2. Select **Move to Exchange** tab

> **NOTE**
>
> This tab is only shown when GFI MailEssentials is installed on Microsoft® Exchange 2010 server.

3. Click **Specify user account...** to specify the dedicated user.
4. Select one of the following options:

Option	Description
Move spam using an automatically created user	Let GFI MailEssentials automatically create a user with all the required rights.
Move spam using the following user account	Use a manually created user. Specify the credentials (**Domain\username** and **Password**) of a dedicated user and click **Set access rights** to assign the required rights to the specified user.

> **NOTE**
>
> The manually specified user credentials must be dedicated to this feature only. Username, password and other properties must not be changed from Microsoft® Exchange or Active Directory, else feature will not work.

5. Click **Finish** to apply settings.
6. Click **OK**.

12.8 Synchronizing configuration data

When GFI MailEssentials is installed on multiple servers, it is important to keep configuration data synchronized between servers.

GFI MailEssentials enables this process through two features that keep multiple GFI MailEssentials installations synchronized:

- Anti-spam synchronization agent - This service automates the process of keeping settings synchronized between separate installations using the Microsoft® BITS service.
- Configuration Export/Import Tool - This application enables the manual export of GFI MailEssentials configuration settings and import to other installations.

12.8.1 Anti-spam synchronization agent

How it works

The Anti-Spam Synchronization Agent works as follows:

1. A server machine hosting GFI MailEssentials is configured as the master server.

2. The other server machines, where GFI MailEssentials is installed, are configured as slave servers.

3. The slave servers upload an archive file, containing settings, to an IIS virtual folder hosted on the master server via the Microsoft® BITS service.

4. When the master server collects all slave servers data, the data is extracted from the individual archives and merged into a central archive file.

5. The slave servers download this central archive file and take care of extracting it and updating the local GFI MailEssentials installation to make use of the new settings.

NOTE

The servers that collaborate in the synchronization of settings must all have the same version of GFI MailEssentials .

NOTE

The files uploaded and downloaded by the synchronization agent are compressed to limit the traffic on the network.

Step 1: Configuring the Synchronization Agent virtual directory on the master server

Important notes

1. Only one server can be configured as master server at any one time.

2. To configure a server as a master server, it must meet one of the following system specifications:

   - Microsoft®Windows Server 2008 with SP1 or later and IIS 7.0, with BITS server extensions installed. Refer to: http://go.gfi.com/?pageid=ME_InstallBITS2003
   - Microsoft® Windows Server 2003 with SP1 or later and IIS 6.0, with BITS server extension installed. Refer to: http://go.gfi.com/?pageid=ME_InstallBITS2008

3. An IIS virtual directory should be created on the master server only.

Virtual directory configuration

In Internet Information Services (IIS) Manager, configure a shared virtual directory on the default website of the master server as described below.

IIS 7.0

a. Load the **Internet Information Services (IIS) Manager** console, right click on the default website and select **Add Virtual Directory**.

b. In the **Add Virtual Directory** dialog, key in `MESynchAgent` as an alias for the virtual directory.

c. Specify a path where to store the contents for this virtual directory and click **OK** to add the virtual directory.

> **NOTE**
>
> Keep note of the configured path for reference.

d. Select **MESynchAgent** virtual directory and from the Features View, double click **SSL Settings**.

e. Disable the **Require SSL** checkbox and click **Apply**.

f. Return to the Features View of the newly added virtual directory and double click **Authentication**.

g. Ensure that only **Basic Authentication** is enabled, while the other options are disabled.

h. Right click **Basic Authentication** and click **Edit…** to specify the **Default Domain** and **Realm** of the username and password used for authentication by the slave machines. Click **OK** and **Apply**.

i. Return to the Features View of **MESynchAgent** virtual directory and double click **BITS Uploads**.

j. Select **Allow clients to upload files** and select **Use default settings from parent**. Click **Apply**.

IIS 6.0

a. From **Internet Information Services (IIS) Manager** console, right click on the default website and select **New > Virtual Directory**.

b. In the **Virtual Directory Creation Wizard** key in `MESynchAgent` as an alias for the virtual directory and click **Next**.

c. Specify a path where to store the contents for this virtual directory and click **Next**.

> **NOTE**
>
> Keep note of the configured path for reference.

d. Select **Read** and **Write** checkboxes and uncheck all other checkboxes. Click **Next** and click **Finish**.

e. Right click **MESynchAgent** virtual directory and select **Properties**.

f. Select **Directory Security** tab and in the **Authentication and access control** group click **Edit**.

g. In **Authenticated access** group check **Basic Authentication** and specify **Default domain** and **Realm** of the username and password used for authentication by the slave machines.

> **NOTE**
>
> Ensure that all other checkboxes are unchecked.

h. Click **OK**.

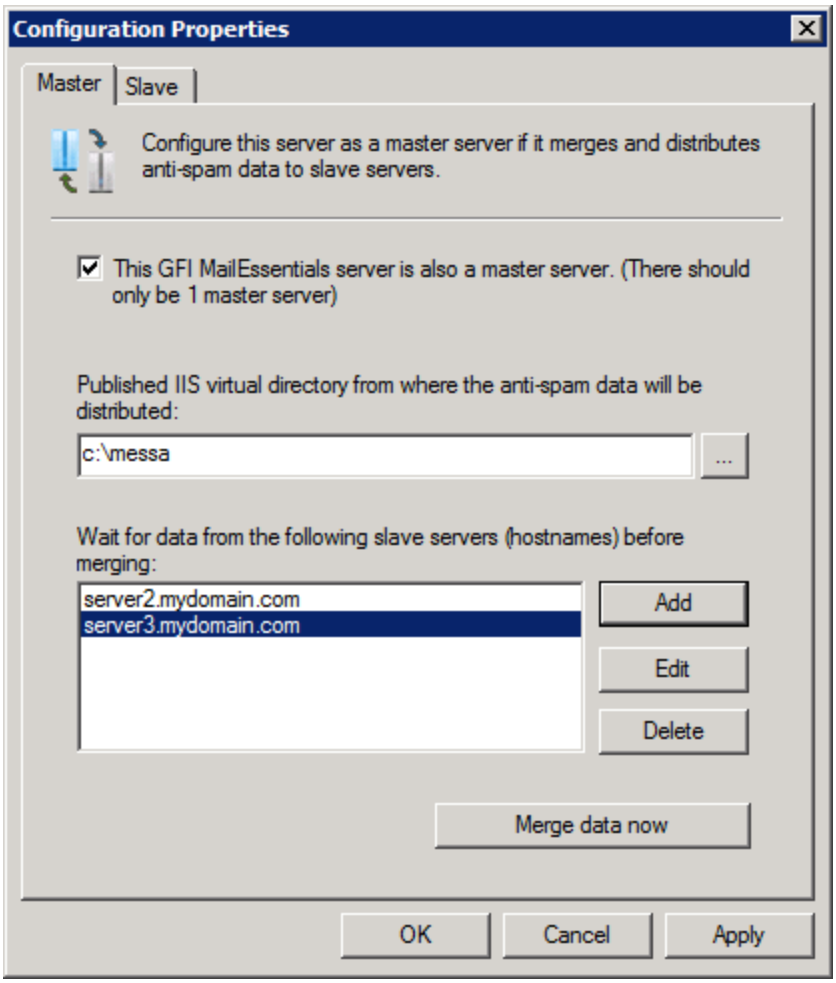
i. Select the **BITS Server Extension** tab and select **Allow clients to transfer data to this virtual directory**.

j. Click **OK** to close the virtual directory dialog properties.

Step 2: Configure the GFI MailEssentials master server

1. From the master server, go to <*GFI MailEssentials installation path*>\GFI\MailEssentials\`AntiSpam\` and open **mesentcfg.msc**.

2. Right click **Anti-Spam Synchronization Agent > Configuration** and select **Properties**.


Configuration Properties
Master
Slave
Configure this server as a master server if it merges and distributes anti-spam data to slave servers.
This GFI MailEssentials server is also a master server. (There should only be 1 master server)
Published IIS virtual directory from where the anti-spam data will be distributed:
c:\messa
...
Wait for data from the following slave servers (hostnames) before merging:
server2.mydomain.com
server3.mydomain.com
Add
Edit
Delete
Merge data now
OK
Cancel
Apply

Screenshot 141: Configuring a master server

3. From the **Master** tab, select **This GFI MailEssentials Configuration server is also a master server** and key in the full path of the folder configured to hold the contents of the **MESynchAgent** virtual directory.

4. Click **Add** and enter the hostname of the slave server. Click **OK** to add it to the list. Repeat this step and add all other slave servers.

NOTE

Ensure that you configure all the machines in this list as slave servers, else the synchronization agent on the master server will not merge the data.

NOTE

A master server can also be a slave server at the same time. In this case the server will merge its own data to the ones uploaded by the other slave servers. For this to work it is required to add the master server hostname to the list of slave servers as well.

5. If required, select a slave server from the list and click **Edit** or **Delete** to edit or delete it.

6. Click **OK**.

Step 3: Configure slave servers

Important notes

1. To configure a server as a slave server, it must meet one of the following system specifications:

   - Microsoft® Windows Server 2008
   - Microsoft® Windows Server 2003 - It is recommend that you download the BITS 2.0 client update from:

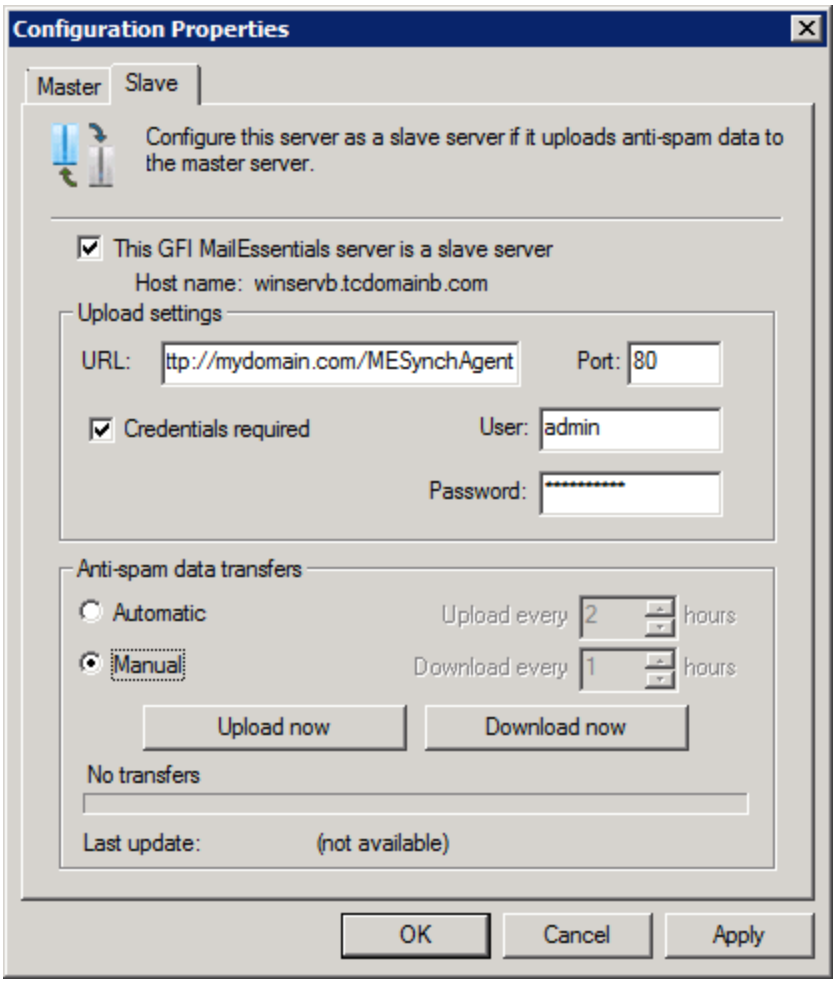
     http://go.gfi.com/?pageid=ME_BITS2003Update

2. Slave servers automatically upload an archive file, containing settings to the IIS virtual directory on the master server, so no virtual directory should be created on slave servers.

Slave server configuration

1. From the slave server, go to <*GFI MailEssentials installation path*>\GFI\MailEssentials\`AntiSpam\` and open **mesentcfg.msc**.

2. Right click **Anti-Spam Synchronization Agent > Configuration** node and select **Properties**.



Screenshot 142: Configuring a slave server

3. From the **Slave** tab, select **This GFI MailEssentials server is a slave server**.

4. In the URL field, specify the full URL to the virtual directory hosted on the master server in the following format:

```
http://<master server domain name>/MESynchAgent
```

- Example: `http://mydomain.com/MESynchAgent`

5. In the **Port** field specify the port used by the master server to accept HTTP communications.

> **NOTE**
>
> By default the port value is set to **80** which is the standard port used for HTTP.

6. Select **Credentials required** and key in credentials used to authenticate with the master server.

7. Select:

Option	Description
Automatic	Synchronization occurs automatically at a set interval. In the **Upload every** field specify the upload interval in hours that determines how often the slave server will upload its settings to the master server. In the **Download every** field specify the download interval in hours which determines how often the slave server checks for updates on the master server and downloads them. Important notes about setting the interval: » The hourly interval for upload and download cannot be set to the same value. » The hourly interval can be set to any value between 1 and 240 hours. » It is recommended that the download interval is configured to a smaller value than the upload interval. » It also recommended to use the same interval for all slave servers. Example: Set download interval to 3 hours and upload interval to 4 hours. This way downloads are more frequent than uploads.
Manual	Upload and download the settings archive file manually. To upload the settings of the slave server to the master server click **Upload now**. To download the updated merged settings from the master server, click **Download now**.

8. Click **OK**.

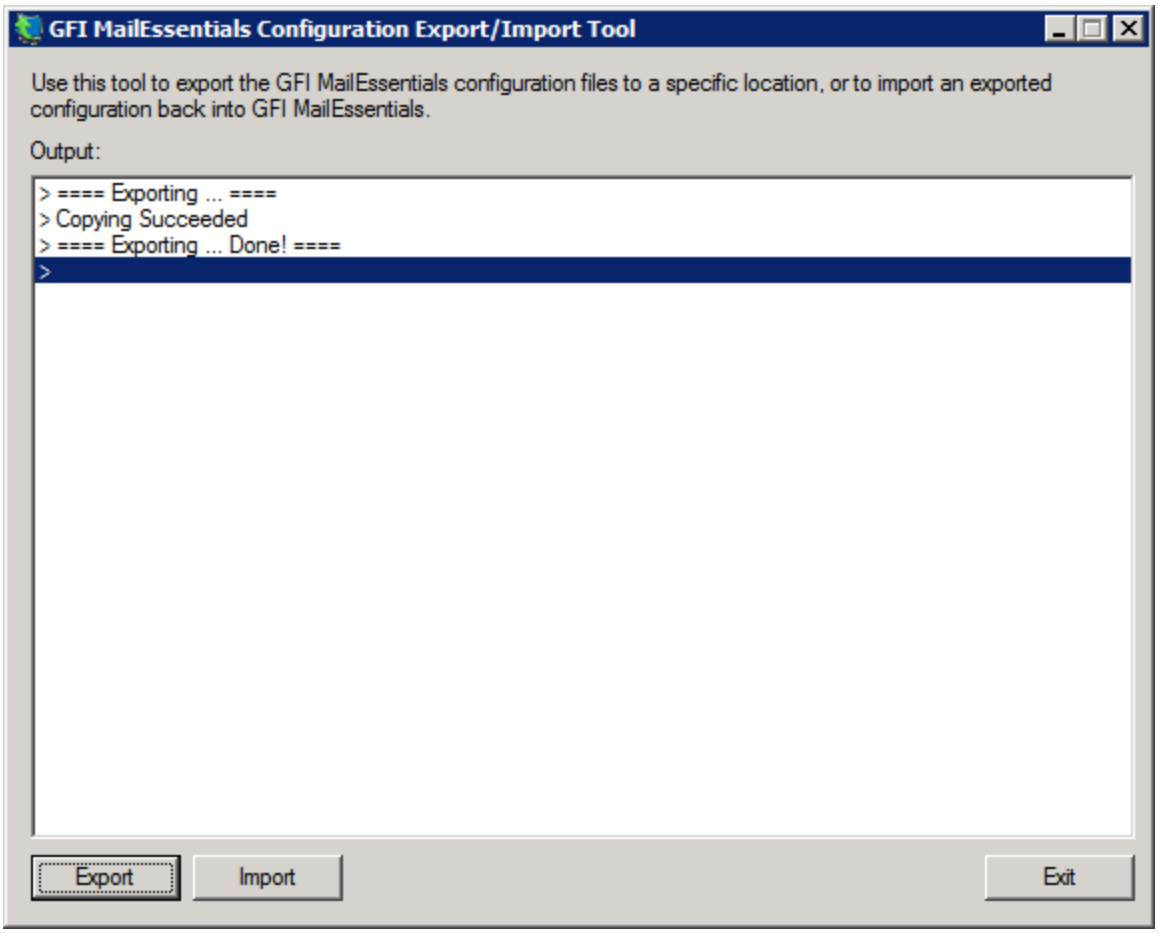
12.8.2 Exporting and importing settings manually

GFI MailEssentials includes a Configuration Export/Import tool to export settings from one installation and import them in another.

> **NOTE**
>
> Settings can also be imported and/or exported from command line. For more information, refer to Export/Import settings via command line (page 249).

Step 1: Export existing settings

1. Go to *<GFI MailEssentials installation path>*`\GFI\MailEssentials\` and launch **meconfigmgr.exe**.


GFI MailEssentials Configuration Export/Import Tool
Use this tool to export the GFI MailEssentials configuration files to a specific location, or to import an exported configuration back into GFI MailEssentials.
Output:
> ==== Exporting ... ====
> Copying Succeeded
> ==== Exporting ... Done! ====
>
Export
Import
Exit

Screenshot 143: Configuration Export/Import Tool

> **NOTE**
>
> Duration of the export process depends on the databases' sizes.

4. Click **Export**.
5. From **Browse for Folder** dialog, choose folder where to export configuration settings and click **OK**.
6. On completion, click **Exit**.

Step 2: Copy the exported settings

1. Manually copy the folder where the configuration settings were exported.
2. Paste the folder to the machines where to import the settings.

Step 3: Import settings to new installation

> **IMPORTANT**
>
> When importing settings, the imported files overwrite existing settings (for example, Source DNS settings) and may require reconfiguration of particular network settings and spam actions.

NOTE

Some services are temporarily stopped while performing this operation. This may affect mail flow and/or email scanning.

1. Stop the following services:
   - GFI List Server
   - GFI MailEssentials Enterprise Transfer
   - GFI MailEssentials Legacy Attendant
   - GFI MailEssentials AntiSpam Attendant
   - GFI POP2Exchange
   - IIS Admin service

2. Go to *<GFI MailEssentials installation path>*\GFI\MailEssentials\ and launch **meconfigmgr.exe**.

NOTE

Duration of the import process depends on size of the databases to be imported.

4. Click **Import**, choose folder containing import data and click **OK**.

WARNING

The import process replaces the configuration files with the files found in this folder.

NOTE

Some imported settings may not be appropriate for the installation of GFI MailEssentials may need to be re-configured. This is possible for example, DNS settings, domains list and perimeter servers are different from the server from which settings were exported. Click **Yes** to launch the GFI MailEssentials Post-Installation wizard to reconfigure important settings.

For more information, refer to Post-Installation Wizard (page 36).

It is also recommended to verify the following settings that are not configured during the Post-Installation wizard.

- **Directory Harvesting** - This must be verified when importing to a server that connects to a different Active Directory or with an Active Directory which is located on a different server. For more information, refer to Directory Harvesting (page 107).
- **Spam Actions** - Some spam actions are only available for Microsoft® Exchange environments. If importing settings to a different environment (for example, on an IIS Server), actions will not work. For more information, refer to Spam Actions - What to do with spam emails (page 135).

NOTE

For more information about settings to verify after import refer to:

http://go.gfi.com/?pageid=ME_CheckImportSettings

6. On completion, click **Exit**.
7. GFI MailEssentials automatically attempts to start the services that were stopped in step 1.

IMPORTANT

There may be other services that are stopped when stopping the **IIS Admin service**, such as the **Simple Mail Transfer Protocol (SMTP)** service. Restart these services manually from the Services applet.

12.8.3 Export/Import settings via command line

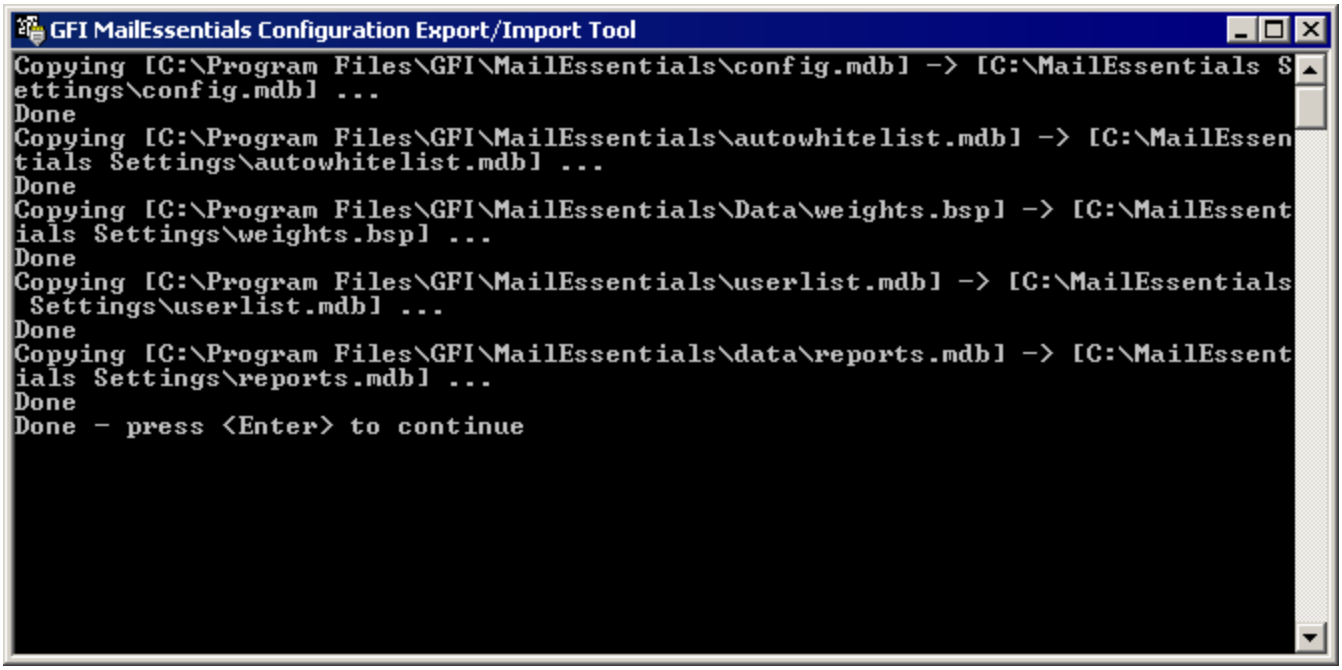
Exporting settings via command line

1. Stop the following GFI MailEssentials services:
   - GFI MailEssentials AS Scan Engine
   - GFI MailEssentials AS Attendant
2. From command prompt, change directory to the GFI MailEssentials installation root folder.
3. Key in:

```
meconfigmgr /export:"c:\MailEssentials Settings" /verbose /replace
```

Where:

- "C:\MailEssentials Settings" - location where to export files. Replace with the desired destination path.
- /verbose - instructs the tool to display progress while copying the files.
- /replace - instructs the tool to overwrite existing files in the destination folder.


GFI MailEssentials Configuration Export/Import Tool
Copying [C:\Program Files\GFI\MailEssentials\config.mdb] -> [C:\MailEssentials Settings\config.mdb] ...
Done
Copying [C:\Program Files\GFI\MailEssentials\autowhitelist.mdb] -> [C:\MailEssentials Settings\autowhitelist.mdb] ...
Done
Copying [C:\Program Files\GFI\MailEssentials\Data\weights.bsp] -> [C:\MailEssentials Settings\weights.bsp] ...
Done
Copying [C:\Program Files\GFI\MailEssentials\userlist.mdb] -> [C:\MailEssentials Settings\userlist.mdb] ...
Done
Copying [C:\Program Files\GFI\MailEssentials\data\reports.mdb] -> [C:\MailEssentials Settings\reports.mdb] ...
Done
Done - press <Enter> to continue

Screenshot 144: Exporting settings via command line

4. Restart the services stopped in step 1.

Importing settings via command line

1. Stop the following services:
   - GFI List Server
   - GFI MailEssentials Enterprise Transfer
   - GFI MailEssentials Legacy Attendant
   - GFI MailEssentials AntiSpam Attendant
   - GFI POP2Exchange
   - IIS Admin service
2. From command prompt, change directory to the GFI MailEssentials installation root folder.
3. Key in:

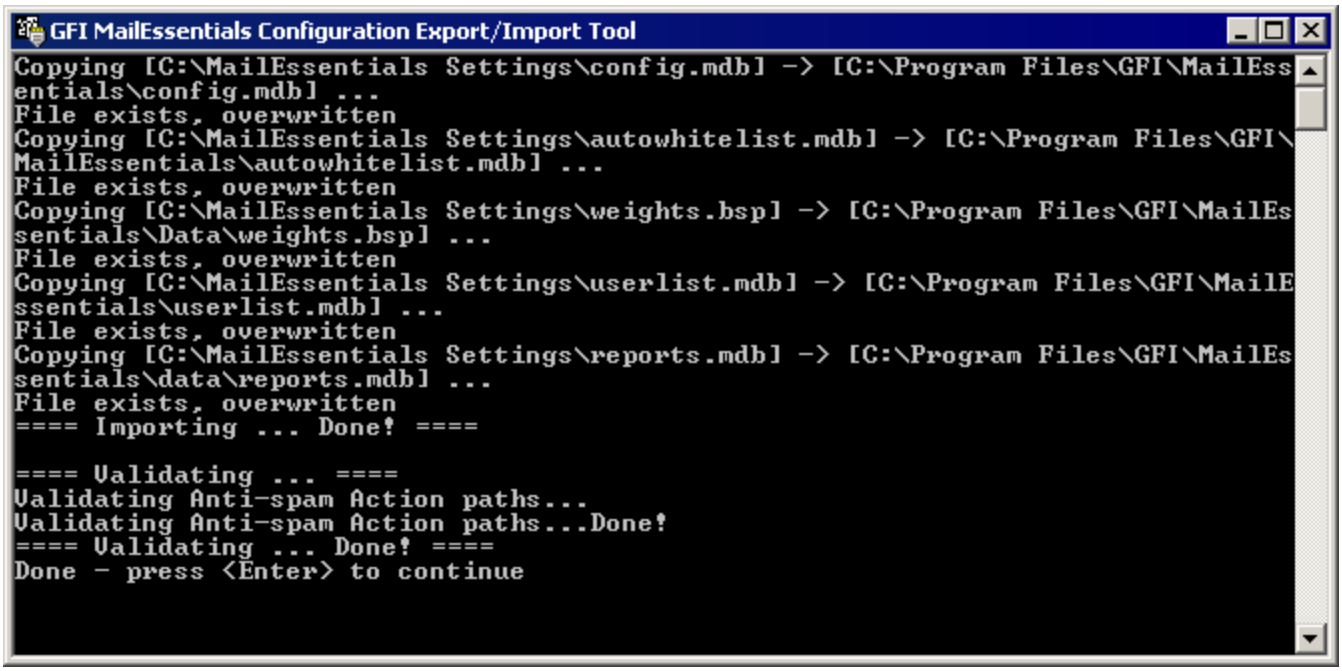
```
meconfigmgr /import:"c:\MailEssentials Settings" /verbose /replace
```

Where:

- "C:\MailEssentials Settings" - location where the files to import are located. Replace with the path where files to be imported are located.
- /verbose - instructs the tool to display progress while copying the files.
- /replace - instructs the tool to overwrite existing files in the destination folder.

WARNING

The import process replaces the configuration files with the files found in this folder.


GFI MailEssentials Configuration Export/Import Tool
Copying [C:\MailEssentials Settings\config.mdb] -> [C:\Program Files\GFI\MailEss
entials\config.mdb] ...
File exists, overwritten
Copying [C:\MailEssentials Settings\autowhitelist.mdb] -> [C:\Program Files\GFI\
MailEssentials\autowhitelist.mdb] ...
File exists, overwritten
Copying [C:\MailEssentials Settings\weights.bsp] -> [C:\Program Files\GFI\MailEs
sentials\Data\weights.bsp] ...
File exists, overwritten
Copying [C:\MailEssentials Settings\userlist.mdb] -> [C:\Program Files\GFI\MailE
ssentials\userlist.mdb] ...
File exists, overwritten
Copying [C:\MailEssentials Settings\reports.mdb] -> [C:\Program Files\GFI\MailEs
sentials\data\reports.mdb] ...
File exists, overwritten
==== Importing ... Done! ====
==== Validating ... ====
Validating Anti-spam Action paths...
Validating Anti-spam Action paths...Done!
==== Validating ... Done! ====
Done - press <Enter> to continue

Screenshot 145: Importing settings via command line

4. Restart the services stopped in step 1.

NOTE

Some imported settings may not be appropriate for the installation of GFI MailEssentials may need to be re-configured. This is possible for example, DNS settings, domains list and perimeter servers are different from the server from which settings were exported. Click **Yes** to launch the GFI MailEssentials Post-Installation wizard to reconfigure important settings.

For more information, refer to Post-Installation Wizard (page 36).

It is also recommended to verify the following settings that are not configured during the Post-Installation wizard.

- **Directory Harvesting** - This must be verified when importing to a server that connects to a different Active Directory or with an Active Directory which is located on a different server. For more information, refer to Directory Harvesting (page 107).
- **Spam Actions** - Some spam actions are only available for Microsoft® Exchange environments. If importing settings to a different environment (for example, on an IIS Server), actions will not work. For more information, refer to Spam Actions - What to do with spam emails (page 135).

NOTE

For more information on the settings to verify after import, refer to:

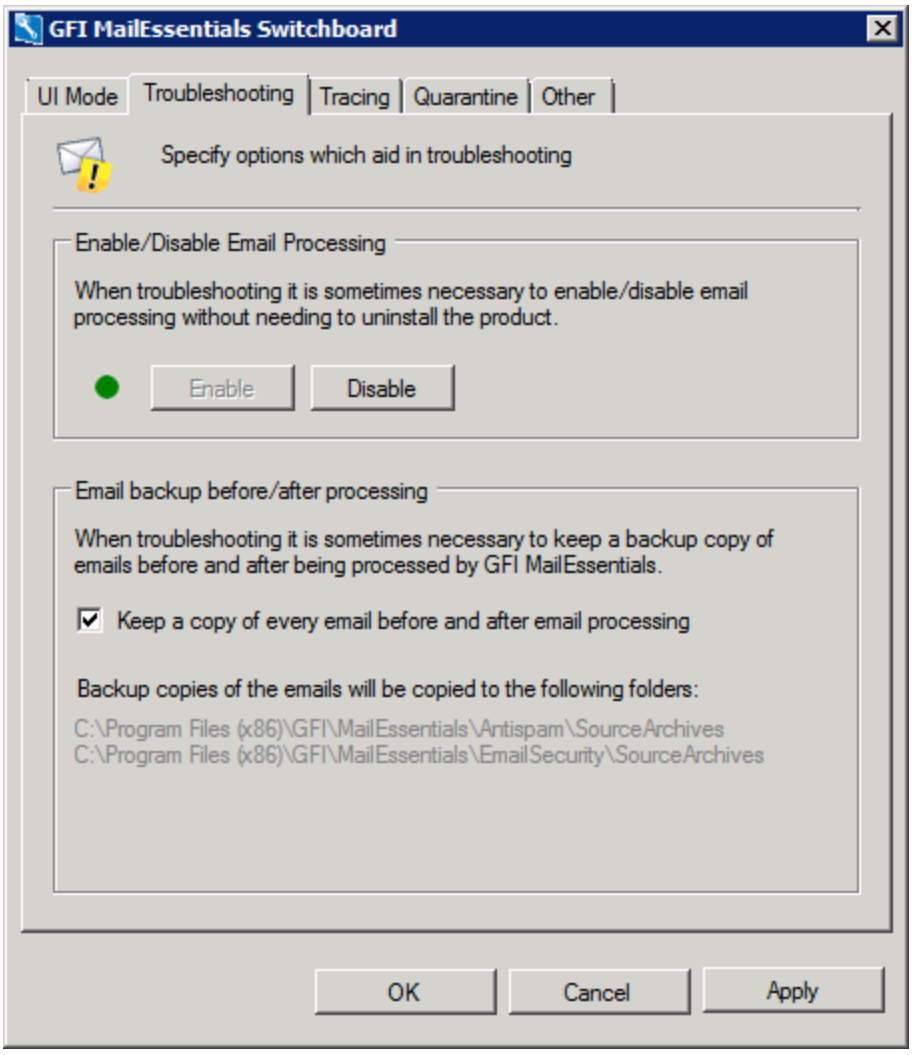
http://go.gfi.com/?pageid=ME_CheckImportSettings

12.9 Disabling email processing

Disabling email processing disables all protection offered by GFI MailEssentials and enables all emails (including spam and malicious emails) to get to your user's mailboxes. Email processing is typically disabled only for troubleshooting purposes.

To enable/disable GFI MailEssentials from processing emails:

1. Launch the GFI MailEssentials Switchboard from **Start > Programs > GFI MailEssentials > Switchboard** and select **Troubleshooting** tab.


GFI MailEssentials Switchboard
UI Mode
Troubleshooting
Tracing
Quarantine
Other
Specify options which aid in troubleshooting
Enable/Disable Email Processing
When troubleshooting it is sometimes necessary to enable/disable email processing without needing to uninstall the product.
Enable
Disable
Email backup before/after processing
When troubleshooting it is sometimes necessary to keep a backup copy of emails before and after being processed by GFI MailEssentials.
Keep a copy of every email before and after email processing
Backup copies of the emails will be copied to the following folders:
C:\Program Files (x86)\GFI\MailEssentials\Antispam\SourceArchives
C:\Program Files (x86)\GFI\MailEssentials\EmailSecurity\SourceArchives
OK
Cancel
Apply

Screenshot 146: The GFI MailEssentials Switchboard: Troubleshooting

2. Click **Enable** or **Disabled** to enable or disable email processing

NOTE

Some services are temporarily stopped while performing this operation. This may affect mail flow and/or email scanning.

3. In the **Service Restart Required** dialog, click **Yes** to restart services.

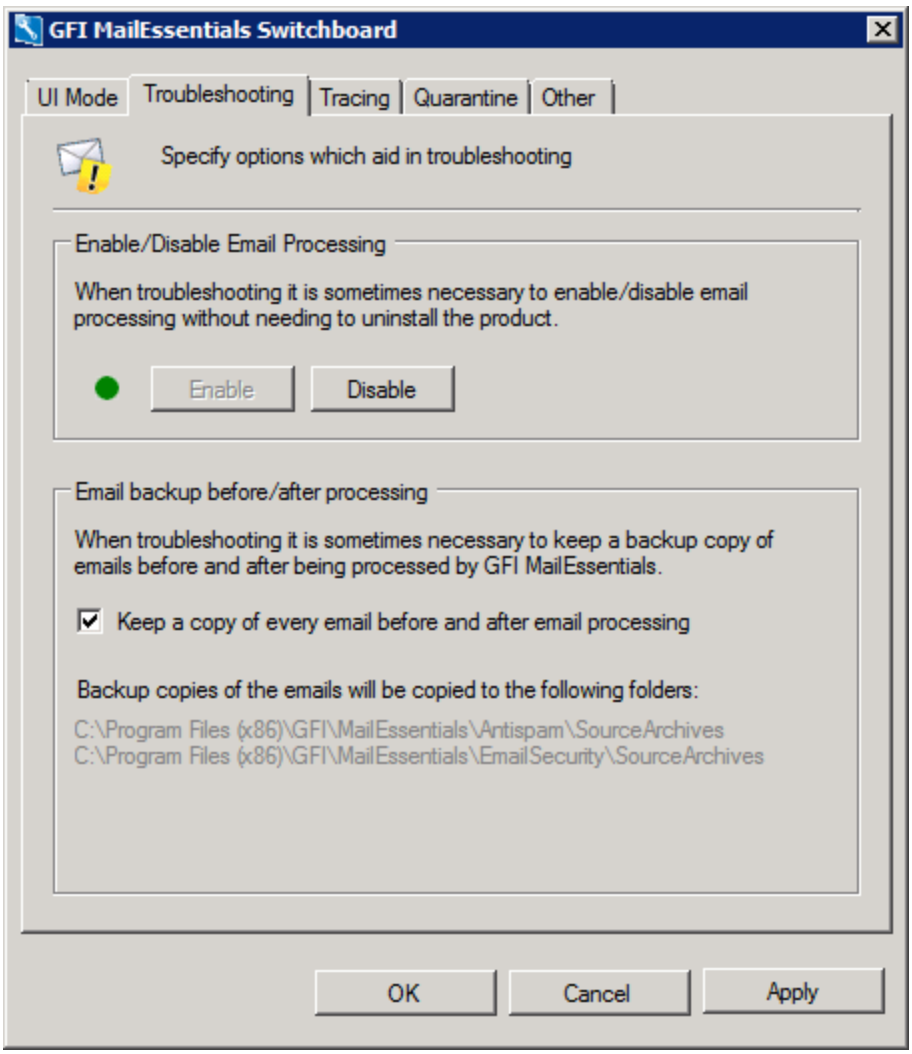
4. Click **OK**.

12.10 Email backup before and after processing

IMPORTANT

Use this option for troubleshooting purposes only.

1. Launch the GFI MailEssentials Switchboard from **Start > Programs > GFI MailEssentials > Switchboard** and select **Troubleshooting** tab.


GFI MailEssentials Switchboard
UI Mode
Troubleshooting
Tracing
Quarantine
Other
Specify options which aid in troubleshooting
Enable/Disable Email Processing
When troubleshooting it is sometimes necessary to enable/disable email processing without needing to uninstall the product.
Enable
Disable
Email backup before/after processing
When troubleshooting it is sometimes necessary to keep a backup copy of emails before and after being processed by GFI MailEssentials.
Keep a copy of every email before and after email processing
Backup copies of the emails will be copied to the following folders:
C:\Program Files (x86)\GFI\MailEssentials\Antispam\SourceArchives
C:\Program Files (x86)\GFI\MailEssentials\EmailSecurity\SourceArchives
OK
Cancel
Apply

Screenshot 147: The GFI MailEssentials Switchboard: Troubleshooting

2. Select/unselect **Keep a copy of every email before and after email processing** checkbox to store a copy of each email processed.

All emails are stored in the following locations:

- *<GFI MailEssentials installation path>*\GFI\MailEssentials\AntiSpam\SourceArchives\
- *<GFI MailEssentials installation path>*\GFI\MailEssentials\EmailSecurity\SourceArchives\

> **NOTE**
>
> Some services are temporarily stopped while performing this operation. This may affect mail flow and/or email scanning.

3. Click **OK**.

4. In the **Service Restart Required** dialog, click **Yes** to restart services.

5. Click **OK**.

12.11 Remoting ports

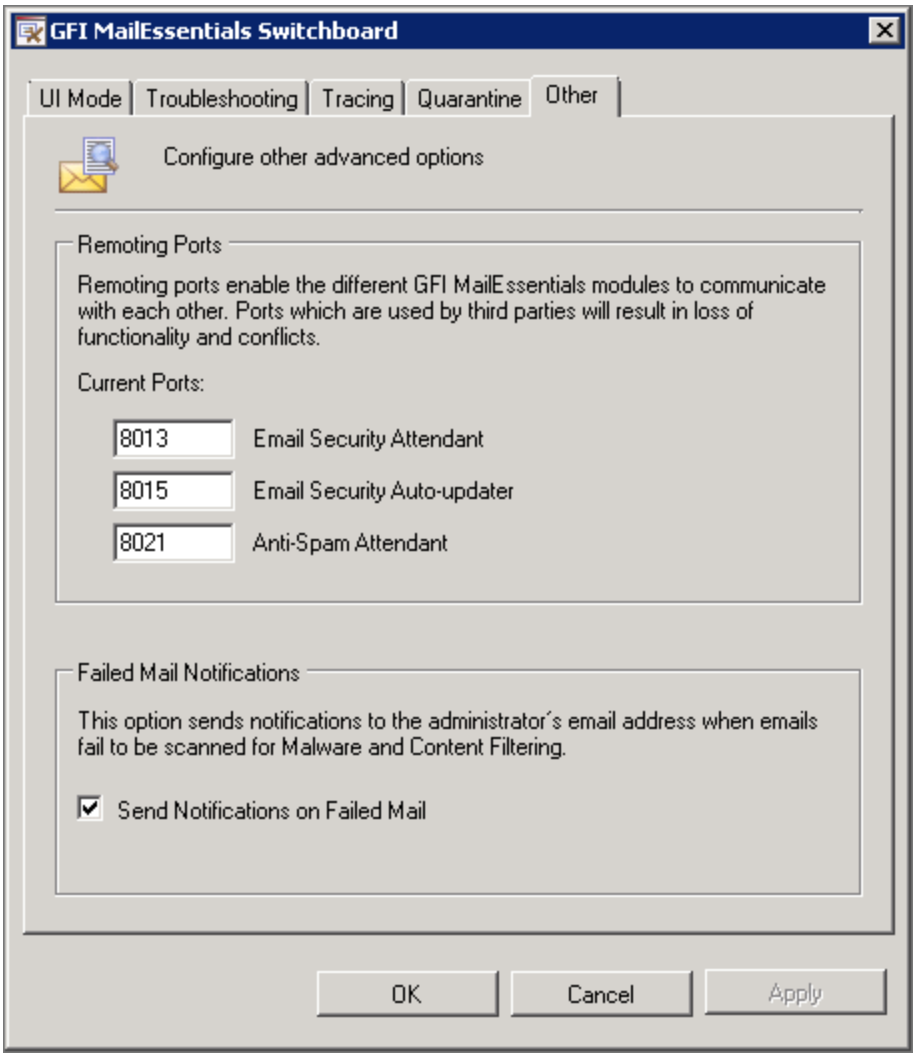
Remoting ports enable modules in GFI MailEssentials to communicate with each other. By default, GFI MailEssentials uses ports:

- 8013
- 8015
- 8021

Ensure that no other applications (except GFI MailEssentials) are listening on these ports. If these ports are used by some other application, change these ports to allow GFI MailEssentials to use alternate ports.

To change the Remoting ports:

1. Launch the GFI MailEssentials Switchboard from **Start > Programs > GFI MailEssentials > Switchboard** and select **Other** tab.


GFI MailEssentials Switchboard
UI Mode
Troubleshooting
Tracing
Quarantine
Other
Configure other advanced options
Remoting Ports
Remoting ports enable the different GFI MailEssentials modules to communicate with each other. Ports which are used by third parties will result in loss of functionality and conflicts.
Current Ports:
8013
Email Security Attendant
8015
Email Security Auto-updater
8021
Anti-Spam Attendant
Failed Mail Notifications
This option sends notifications to the administrator's email address when emails fail to be scanned for Malware and Content Filtering.
Send Notifications on Failed Mail
OK
Cancel
Apply

Screenshot 148: Changing Remoting ports

2. In the **Remoting Ports** area, change the number of the Remoting port to a one that is not utilized by other applications.

3. Click **Apply**.

> **NOTE**
>
> Some services are temporarily stopped while performing this operation. This may affect mail flow and/or email scanning.

4. Click **Yes** to restart the displayed services.

5. Click **OK**.

12.12 Monitoring Virus Scanning API

When GFI MailEssentials is installed on the Microsoft® Exchange machine, you can monitor Virus Scanning API performance using the Performance Monitor MMC.

NOTE

Information Store Protection (VSAPI) is not supported on Microsoft® Exchange Server 2013 because VSAPI was removed from Microsoft® Exchange Server 2013 by Microsoft.

12.12.1 Performance counter in Windows 2003 Server

To add and view, the performance monitor counter in Windows 2003 Server, follow these steps:

1. Go to **Start > Control Panel**.
2. In the Control Panel window, double-click **Administrative Tools**.
3. Double-click **Performance**, to start the **Performance monitor** MMC.
4. From the **System Monitor** viewing pane, click **Add** to load the **Add Counters** dialog.
5. From the **Performance object** dropdown list, select **MSExchangeIS**.
6. Click **Select counters from list**.
7. Select any **Virus Scan** counter you need to add. For more information, refer to Performance monitor counters (page 258).
8. Click **Add**.
9. Repeat steps 7 and 8 to add all the performance counters needed.
10. Click **Close**.

The counters of added processes are now displayed in the Performance Monitor.

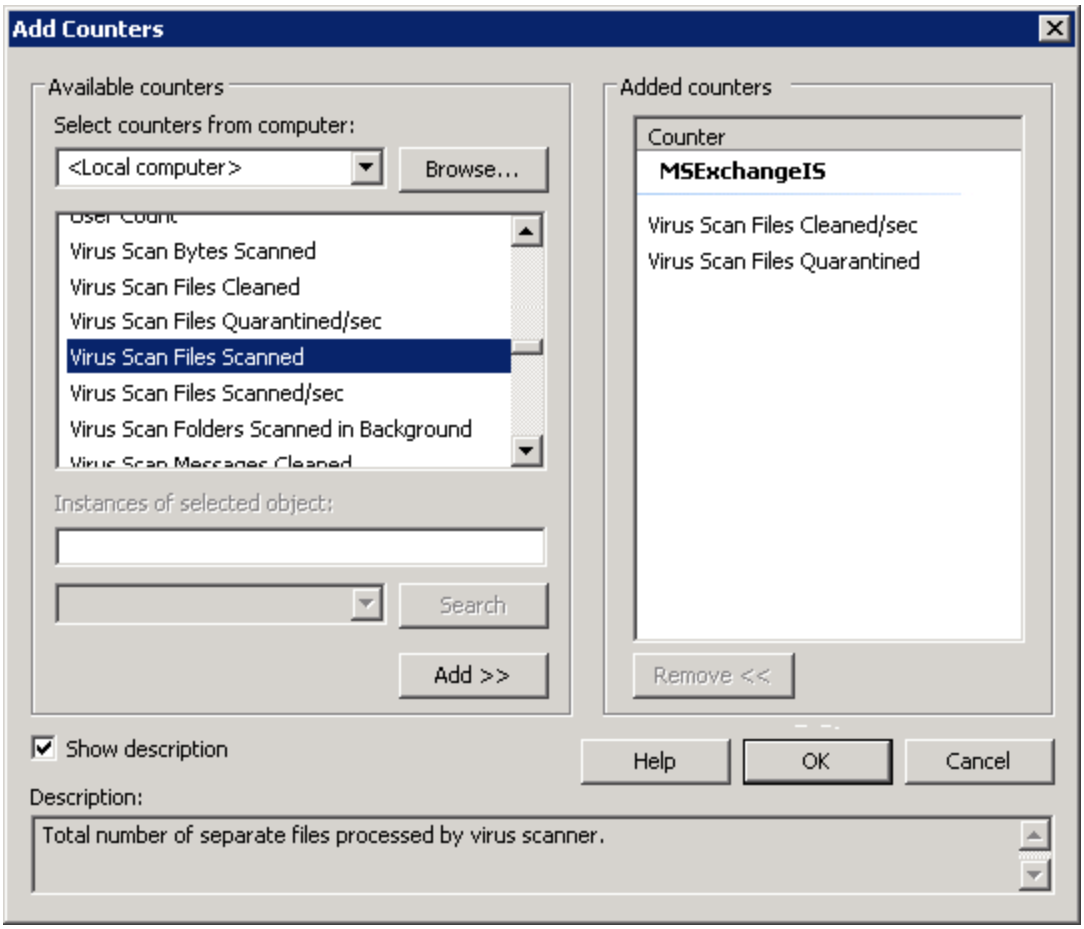
12.12.2 Performance counter in Windows 2008 Server

NOTE

In a Microsoft® Exchange Server 2007/2010 environment, the VSAPI performance monitor counters are only available on machines with the Mailbox Server Role installed.

To add and view, the performance monitor counter in Windows 2008 Server, follow these steps:

1. Go to **Start > Control Panel > Administrative Tools > Reliability and Performance Monitor**.
2. In the monitor dialog, expand **Monitoring Tools** and select **Performance Monitor**.
3. From the viewing pane, click **Add** to load the **Add Counters** dialog.



Screenshot 149: Adding VSAPI performance monitor counters in Windows 2008 Server

4. From the **Select counters from computer** dropdown list, select the computer to monitor.

5. From the list of available counters, expand **MSExchangeIS**.

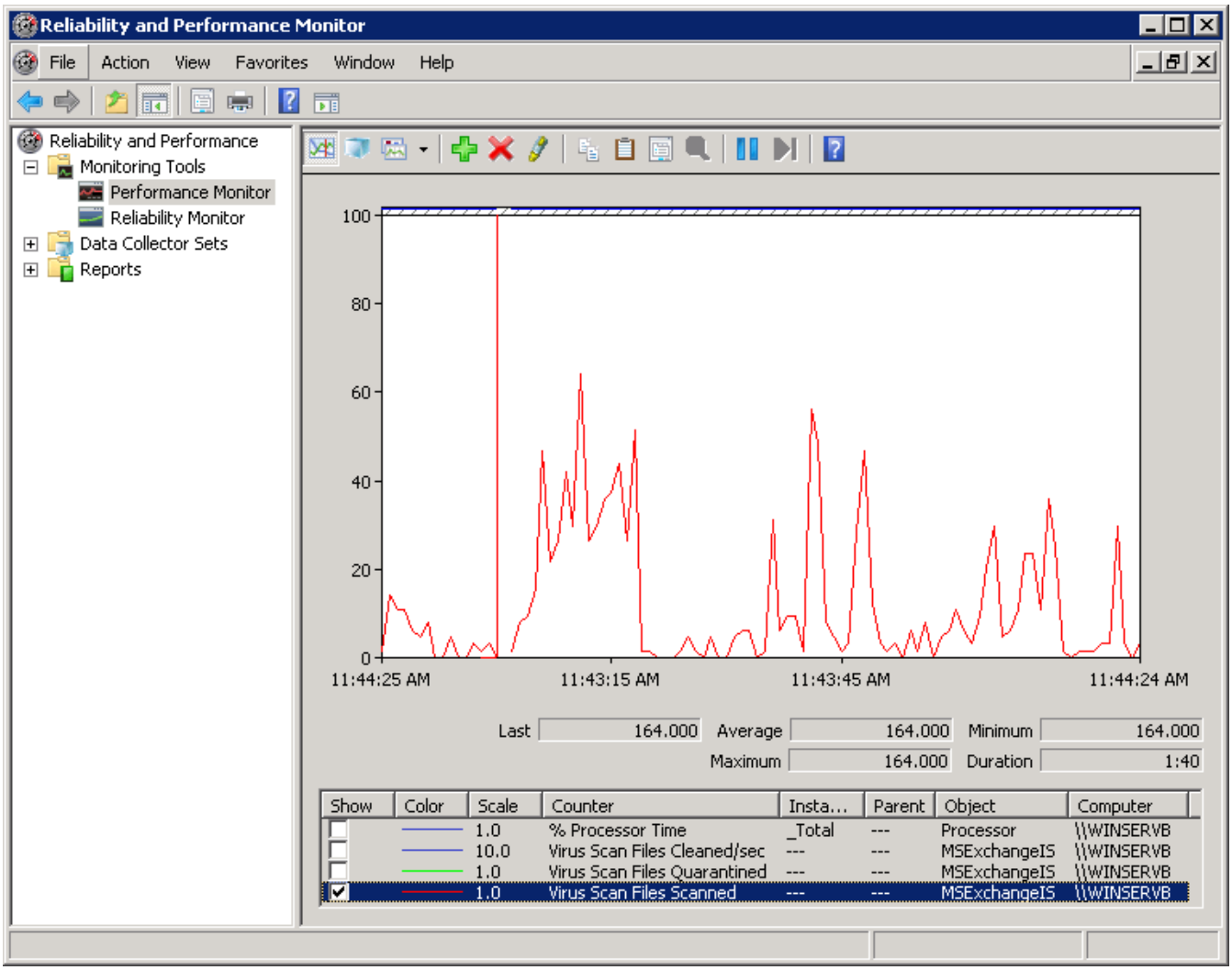
6. Select any **Virus Scan** counter you need to add. For more information, refer to Performance monitor counters (page 258).

7. Click **Add**.

8. Repeat steps 6 and 7 for each process to monitor.

9. Click **Ok** to apply changes.

The counters of added processes are now displayed in the Performance Monitor.



Screenshot 150: Monitoring Virus Scan Files Scanned in Windows Server 2008 Performance Monitor

12.12.3 Performance monitor counters

The following VSAPI Performance Monitor counters are available:

Performance Counter	Description
Virus Scan Messages Processed	A cumulative value of the total number of top-level messages that are processed by the virus scanner.
Virus Scan Messages Processed/sec	Represents the rate at which top-level messages are processed by the virus scanner.
Virus Scan Messages Cleaned	Total number of top-level messages that are cleaned by the virus scanner.
Virus Scan Messages Cleaned/sec	Rate at which top-level messages are cleaned by the virus scanner.
Virus Scan Messages Quarantined	Total number of top-level messages that are put into quarantine by the virus scanner.
Virus Scan Messages Quarantined/sec	Rate at which top-level messages are put into quarantine by the virus scanner.
Virus Scan Files Scanned	Total number of separate files that are processed by the virus scanner.
Virus Scan Files Scanned/sec	Rate at which separate files are processed by the virus scanner.
Virus Scan Files Cleaned	Total number of separate files that are cleaned by the virus scanner.
Virus Scan Files Cleaned/sec	Rate at which separate files are cleaned by the virus scanner.
Virus Scan Files Quarantined	Total number of separate files that are put into quarantine by the virus scanner.
Virus Scan Files Quarantined/sec	Rate at which separate files are put into quarantine by the virus scanner.

Performance Counter	Description
Virus Scan Bytes Scanned	Total number of bytes in all of the files that are processed by the virus scanner.
Virus Scan Queue Length	Current number of outstanding requests that are queued for virus scanning.
Virus Scan Folders Scanned in Background	Total number of folders that are processed by background scanning.
Virus Scan Messages Scanned in Background	Total number of messages that are processed by background scanning.

13 Troubleshooting and support

13.1 Introduction

This chapter explains how to resolve any issues encountered during installation of GFI MailEssentials. The main sources of information available to solve these issues are:

- This manual - most issues can be solved through the information in this section.
- GFI Knowledge Base articles
- Web forum
- Contacting GFI Technical Support

13.2 Common issues

Issue encountered	Solution
Dashboard shows no email is being processed; or, Only inbound or outbound emails are being processed	1. Ensure that GFI MailEssentials is not disabled from scanning emails. For more information, refer to Disabling email processing (page 252). 2. Check for multiple Microsoft® IIS SMTP virtual servers and ensure that GFI MailEssentials is bound to the correct virtual server. For more information, refer to SMTP Virtual Server bindings (page 223). 3. MX record for domain not configured correctly. Ensure that the MX record points to the IP address of the server running GFI MailEssentials. 4. If inbound emails are passing through another gateway, ensure that the mail server running on the other gateway forwards inbound emails through GFI MailEssentials. 5. Ensure that outbound emails are configured to route through GFI MailEssentials. For more information, refer to Installing on an email gateway or relay/perimeter server (page 28). 6. Verify that the SMTP virtual server used by Microsoft® Exchange Server for outbound emails is the same SMTP server GFI MailEssentials is bound to. For more information how to solve this issue refer to: http://go.gfi.com/?pageid=ME_MonitorProcessing
After installing GFI MailEssentials, some emails show a garbled message body when viewed in Microsoft® Outlook	This problem occurs for emails that use one character set for the message header and a different character set for the message body. When such emails are processed by Microsoft® Exchange 2003, the emails will be shown garbled in Microsoft® Outlook. Microsoft® has released a hotfix to resolve this issue. For more information refer to: http://go.gfi.com/?pageid=ME_OutlookCharacters and http://go.gfi.com/?pageid=ME_MessageGarbled
GFI MailEssentials is configured to move mails blocked as SPAM to a subfolder of the users' mailbox. Clients connected to Microsoft® Exchange via POP3 are not able to view mails blocked as SPAM.	Connect to Microsoft® Exchange using IMAP. For more information refer to: http://go.gfi.com/?pageid=ME_POP3ViewSpam
Auto updates fail however manual download via the GFI MailEssentials configuration works fine	Ensure that un-authenticated connections are allowed from the GFI MailEssentials machine to http://update.gfi.com on port 80. For more information refer to: http://go.gfi.com/?pageid=ME_AutoUpdatesFail Also check Proxy Server, if applicable.
Configuration data cannot be imported.	Ensure that the GFI MailEssentials version and build is identical across both source and target installations. For more information how to solve this issue refer to: http://go.gfi.com/?pageid=ME_ExpImpBuild

Issue encountered	Solution
Remote commands do not work	Refer to: http://go.gfi.com/?pageid=ME_RemoteCommands
Processing of emails is very slow	This may occur when there are DNS problems in the network. If DNS is not working correctly, the DNS lookups made by some anti-spam filters in GFI MailEssentials will timeout. For more information refer to: http://go.gfi.com/?pageid=ME_ProcessingSlow
Older data not available in database when using Microsoft® Access.	When **reports.mdb** database exceeds 1.7 GB, the database is automatically renamed to **reports_<date>.mdb** and a new **reports.mdb** database is created. For more information how to solve this issue refer to: http://go.gfi.com/?pageid=ME_ReportDB
The Quarantine interface shows error D10 - **Cannot access the Quarantine Store database. Use a database repair tool (such as esentutl.exe) to repair the database.**	Refer to http://go.gfi.com/?pageid=ME_esentutl for more information how to use esentutl.exe to repair the Quarantine Store database.
Error when receiving emails: **Body type not supported by Remote Host**	This error occurs when emails are relayed from the IIS SMTP server to the Microsoft® Exchange server. This happens because Microsoft® Exchange Server versions 4.0, 5.0, and 5.5 are not able to handle 8-bit MIME messages. For instructions how to turn off 8BITMIME in Windows Server 2003 refer to: http://go.gfi.com/?pageid=ME_TurnOff8bitMIME.
Legitimate emails are moved to the **failedmails** folder	**Cause** When GFI MailEssentials is not able to scan incoming emails, these emails are not delivered to the recipient(s) since they may contain malicious content. GFI MailEssentials moves these emails to the following folder: <*GFI MailEssentials installation path*>\GFI\MailEssentials\EmailSecurity\failedmails\ **Solution** If any legitimate emails are moved to the failedmails folder, these can be manually re-processed for delivery. For more information, refer to Failed emails (page 231). For more information of failed emails, refer to: http://go.gfi.com/?pageid=ME_FailedMails
Do I need to upgrade my license key when upgrading to a new version?	Information on licensing is available on: http://go.gfi.com/?pageid=ME_adminManualEN
Where is the online version of this manual?	The online version of this manual is available from: http://go.gfi.com/?pageid=GFI_Manuals

13.3 Scanning engines & filters

Issue encountered	Solution
Spam is delivered to users mailbox	Follow the checklist below to solve this issue: 1. Check that GFI MailEssentials is not disabled from scanning emails. For more information, refer to Disabling email processing (page 252). 2. Check if all required filters are enabled. For more information, refer to Anti-Spam filters (page 101). 3. Check if local domains are configured correctly. For more information, refer to Local domains (page 222). 4. Check if emails are passing through GFI MailEssentials or if GFI MailEssentials is bound to the correct IIS SMTP Virtual Server. 5. Check if '%TEMP%' location (which by default is the 'C:\Windows\Temp' folder) contains a lot of files. 6. Check if the number of users using GFI MailEssentials exceeds the number of purchased licenses. 7. Check if whitelist is configured correctly. For more information, refer to Whitelist (page 130). 8. Check if actions are configured correctly. For more information, refer to Spam Actions - What to do with spam emails (page 135). 9. Check if Bayesian Analysis filter is configured correctly. For more information, refer to Bayesian Analysis (page 128). For more information how to solve this issue refer to: http://go.gfi.com/?pageid=ME_SpamChecklist
Email Blocklist, Whitelist and/or Content Filtering pages take long to load or appear to hang	Limit the amount of entries in the lists to 10,000.
SpamRazer updates not downloading	1. Ensure that your license key is valid. 2. Ensure that the required ports are open and that your firewall is configured to allow connections from the GFI MailEssentials server. For more information, refer to Firewall port settings (page 27). 3. Ensure that, if applicable, proxy server settings for connection to Internet are correct.
Emails are not being greylisted	To verify the operation of Greylist: **Step 1: Confirm that Greylist is enabled** From the Greylist properties ensure that Enable Greylist is selected. **Step 2: Verify excluded addresses** From the IP and Email exclusions in Greylist properties, ensure that there are no incorrect exclusions (such as *@*.com). **Step 3: Use esentutl.exe to ensure the Greylist database is not corrupted.** For more information refer to: http://go.gfi.com/?pageid=ME_esentutl
Receiving spam emails from my domain.	Some Spam emails contain a fake 'SMTP FROM' email address consisting of the same domain as the recipient. This may seem as if the email is coming from a local user. 1. Enable Sender Policy Framework from within SpamRazer anti-spam filter, to block emails originating from spoofed addresses. For more information, refer to SpamRazer (page 102). 2. Create an SPF record for your domain. For more information refer to http://go.gfi.com/?pageid=ME_CreateSPFRecord. 3. Ensure that SpamRazer is configure to run at a higher priority than the Whitelist module. For more information, refer to Sorting anti-spam filters by priority (page 138).

Issue encountered	Solution
GFI MailEssentials returns the following error: "The file was blocked by the attachment filtering module at file type checking stage. The attachment claimed to be a <filetype 1> which is identified as being an attachment in category <filetype 1>. The file was detected to belong to the category <filetype 2>."	**Cause** An attached file is detected as being a file with multiple file-types. **Solution** For information how to resolve this issue refer to: http://go.gfi.com/?pageid=ME_FiletypeError. **NOTE** The solution to this issue requires changes in the Windows Registry. It is important to follow the steps described in the solution with attention as incorrect configuration can cause serious, system-wide problems.
Emails sent from whitelisted senders are blocked.	1. Whitelisted emails can be blocked if they contain content or attachments that violate the Anti-Malware rules, since these have a higher order of priority than the whitelist. Ensure that blocked emails do not violate Anti-Malware rules. 2. Ensure that the filter priories are set so that the whitelist is above any kind of filter that is catching the desired email. For more information refer to: http://go.gfi.com/?pageid=ME_BlockedWhitelistedSenders
Spam not delivered to Microsoft® Exchange sub folder or Spam is not being delivered to the designated sub-folder in Outlook in a Microsoft® Exchange Server 2010 environment	1. Confirm that this feature is configured correctly. For more information, refer to Move spam to Exchange 2010 folder (page 240). 2. Refer to http://go.gfi.com/?pageid=ME_AutodiscoverIssues for detailed information on how to solve this issue.

13.4 Email Management

Issue encountered	Solution
No disclaimers are added to outbound emails	Disclaimers are only added to outbound emails originating from domains protected by GFI MailEssentials. Disclaimers are not added when: » Emails are sent from domains that are not specified in local domains list. » Emails are sent to domains that are in the local domains list as these will be considered as internal emails. Ensure that all local domains are specified in the Inbound email domains dialog. For more information, refer to Local domains (page 222).
Some characters in disclaimer text are not displayed correctly	Configure Microsoft® Outlook not to use automatic encoding and force GPO to use correct encoding. For more information how to solve this issue refer to: http://go.gfi.com/?pageid=ME_Outlook2003Encoding
Emails sent to the list server are converted to Plain Text	Emails sent to the List server are converted to plain text emails only when the original format of the email is RTF. Send email in HTML format to retain original format
Internal users receive a non-delivery report when sending email to list server when GFI MailEssentials is installed on a Gateway machine	For more information how to use the List Server feature if GFI MailEssentials is installed on a gateway refer to: http://go.gfi.com/?pageid=ME_ListServerGateway
Emails sent from certain users, or sent to certain users are not monitored.	Email monitoring rules do not monitor emails sent from or to the GFI MailEssentials administrator and the email address to which the monitored emails are being sent to. Email monitoring rules are also not applicable for emails sent between internal users of the same information store.

13.5 GFI SkyNet

GFI maintains a comprehensive knowledge base repository, which includes answers to the most common problems. GFI SkyNet always has the most up-to-date listing of technical support questions and patches. In case that the information in this guide does not solve your problems, next refer to GFI SkyNet by visiting: http://kb.gfi.com/.

13.6 Web Forum

User to user technical support is available via the GFI web forum. Access the web forum by visiting: http://forums.gfi.com/.

13.7 Request technical support

If none of the resources listed above enable you to solve your issues, contact the GFI Technical Support team by filling in an online support request form or by phone.

- **Online**: Fill out the support request form and follow the instructions on this page closely to submit your support request on: http://support.gfi.com/supportrequestform.asp
- **Phone**: To obtain the correct technical support phone number for your region visit: http://www.gfi.com/company/contact.htm

> **NOTE**
>
> Before contacting Technical Support, have your Customer ID available. Your Customer ID is the online account number that is assigned to you when first registering your license keys in the GFI Customer Area at: http://customers.gfi.com.

We will answer your query within 24 hours or less, depending on your time zone.

13.8 Documentation

If this manual does not satisfy your expectations, or if you think that this documentation can be improved in any way, let us know via email on: documentation@gfi.com.

14 Appendix 1 - Bayesian Filtering

The Bayesian filter is an anti-spam technology used within GFI MailEssentials. It is an adaptive technique based on artificial intelligence algorithms, hardened to withstand the widest range of spamming techniques available today.

This chapter explains how the Bayesian filter works, how it can be configured and how it can be trained.

NOTE

1. The Bayesian anti-spam filter is disabled by default. It is highly recommended that you train the Bayesian filter before enabling it.

2. GFI MailEssentials must operate for at least one week for the Bayesian filter to achieve its optimal performance. This is required because the Bayesian filter acquires its highest detection rate when it adapts to your email patterns.

How does the Bayesian spam filter work?

Bayesian filtering is based on the principle that most events are dependent and that the probability of an event occurring in the future can be inferred from the previous occurrences of that event.

NOTE

Refer to the links below for more information on the mathematical basis of Bayesian filtering:

http://go.gfi.com/?pageid=ME_BayesianParameterEstimation

This same technique has been adapted by GFI MailEssentials to identify and classify spam. If a snippet of text frequently occurs in spam emails but not in legitimate emails, it would be reasonable to assume that this email is probably spam.

Creating a tailor-made Bayesian word database

Before Bayesian filtering is used, a database with words and tokens (for example $ sign, IP addresses and domains, etc,) must be created. This can be collected from a sample of spam email and valid email (referred to as 'ham').

A probability value is then assigned to each word or token; this is based on calculations that account for how often such word occurs in spam as opposed to ham. This is done by analyzing the users' outbound email and known spam: All the words and tokens in both pools of email are analyzed to generate the probability that a particular word points to the email being spam.

This probability is calculated as per following example:

If the word 'mortgage' occurs in 400 out of 3,000 spam emails and in 5 out of 300 legitimate emails then its spam probability would be 0.8889 (i.e. [400/3000] / [5/300 + 400/3000]).

Creating a custom ham email database

The analysis of ham email is performed on the company's email and therefore is tailored to that particular company.

- **Example:** A financial institution might use the word 'mortgage' many times and would get many false positives if using a general anti-spam rule set. On the other hand, the Bayesian filter, if tailored to your company through an initial training period, takes note of the company's valid outbound email (and recognizes 'mortgage' as being frequently used in legitimate messages), it will have a much better spam detection rate and a far lower false positive rate.

Creating the Bayesian spam database

Besides ham email, the Bayesian filter also relies on a spam data file. This spam data file must include a large sample of known spam. In addition it must also constantly be updated with the latest spam by the anti-spam software. This will ensure that the Bayesian filter is aware of the latest spam trends, resulting in a high spam detection rate.

How is Bayesian filtering done?

Once the ham and spam databases have been created, the word probabilities can be calculated and the filter is ready for use.

On arrival, the new email is broken down into words and the most relevant words (those that are most significant in identifying whether the email is spam or not) are identified. Using these words, the Bayesian filter calculates the probability of the new message being spam. If the probability is greater than a threshold, the message is classified as spam.

NOTE

For more information on Bayesian Filtering and its advantages refer to:

http://go.gfi.com/?pageid=ME_Bayesian

14.0.1 Training the Bayesian Analysis filter

NOTE

The Bayesian Analysis filter can also be trained using Public folders. For more information, refer to Configuring the Bayesian filter (page 128).

It is recommended that the Bayesian Analysis filter is trained through the organization's mail flow over a period of time. It is also possible for Bayesian Analysis to be trained from emails sent or received before GFI MailEssentials is installed by using the Bayesian Analysis wizard. This allows Bayesian Analysis to be enabled immediately.

This wizard analyzes sources of:

- legitimate mail - for example a mailbox' sent items folder
- spam mail - for example a mailbox folder dedicated to spam emails.

Step 1: Install the Bayesian Analysis wizard

The Bayesian Analysis wizard can be installed on:

- A machine that communicates with Microsoft® Exchange - to analyze emails in a mailbox
- A machine with Microsoft Outlook installed - to analyze emails in Microsoft Outlook

1. Copy the Bayesian Analysis wizard setup file **bayesianwiz.exe** to the chosen machine. This is located in:

GFI MailEssentials *installation path\AntiSpam\BSW*

2. Launch **bayesianwiz.exe** and click **Next** in the welcome screen.

Select the installation folder and click **Next**.

4. Click **Next** to start installation.

5. Click **Finish** when installation is complete.

Step 2: Analyze legitimate and spam emails

To start analyzing emails using the Bayesian Analysis wizard:

1. Load the Bayesian Analysis wizard from **Start > Programs > GFI MailEssentials > GFI MailEssentials Bayesian Analysis Wizard**.

2. Click **Next** in the welcome screen.

3. Choose whether to:

- Create a new Bayesian Spam Profile (.bsp) file or update an existing one. Specify the path where to store the file and the filename.
- Update the Bayesian Spam profile used by the Bayesian Analysis filter directly when installing on the same machine as GFI MailEssentials.

Click **Next** to proceed.

4. Select how the wizard will access legitimate emails. Select:

- **Use Microsoft Outlook profile configured on this machine** - Retrieves emails from a Microsoft Outlook mail folder. Microsoft Outlook must be running to use this option.
- **Connect to a Microsoft® Exchange Server mailbox store** - Retrieves emails from a Microsoft® Exchange mailbox. Specify the logon credentials in the next screen.
- **Do not update legitimate mail (ham) in the Bayesian Spam profile** - skip retrieval of legitimate emails. Skip to step 6.

Click **Next** to continue.

5. After the wizard connects to the source, select the folder containing the list of legitimate emails (e.g. the Sent items folder) and click **Next**.

6. Select how the wizard will access the source of spam emails. Select:

- **Download latest Spam profile from GFI website** - Downloads a spam profile file that is regularly updated by collecting mail from leading spam archive sites. An Internet connection is required.
- **Use Microsoft Outlook profile configured on this machine** - Retrieves spam from a Microsoft Outlook mail folder. Microsoft Outlook must be running to use this option.
- **Connect to a Microsoft® Exchange Server mailbox store** - Retrieves spam from a Microsoft® Exchange mailbox. Specify the logon credentials in the next screen.
- **Do not update Spam in the Bayesian Spam profile** - skip retrieval of spam emails. Skip to step 8.

Click **Next** to continue.

7. After the wizard connects to the source, select the folder containing the list of spam emails and click **Next**.

8. Click **Next** to start retrieving the sources specified. This process may take several minutes to complete.

9. Click **Finish** to close the wizard.

Step 3: Import the Bayesian Spam profile

When the wizard is not run on the GFI MailEssentials server, import the Bayesian Spam Profile (.bsp) file to GFI MailEssentials.

1. Move the file to the **Data** folder in the GFI MailEssentials installation path.

2. Restart the **GFI MailEssentials AS Scan Engine** and the **GFI MailEssentials Legacy Attendant** services.

15 Appendix 2 - Lotus Domino

Use this Appendix for information on using GFI MailEssentials with your Lotus Domino installation.

15.1 Lotus Domino incompatibilities

15.1.1 Internal memos/emails are not scanned

GFI MailEssentials does not scan internal memos/emails sent by Lotus Domino since the Lotus Domino's sender/receiver format is not in a compatible format. When internal memos/emails are passed into GFI MailEssentials, these end up in the queue and are not processed.

NOTE

Do not pass internal memos/emails through GFI MailEssentials.

15.1.2 GFI MailEssentials List Server will not work with Lotus Domino

Creating Newsletters or discussion lists will not work for the internal domain of Lotus Domino. This option should not be used. If used, Lotus Domino users will not be able to send emails to the list.

15.2 GFI MailEssentials Installation Guide for Lotus Domino

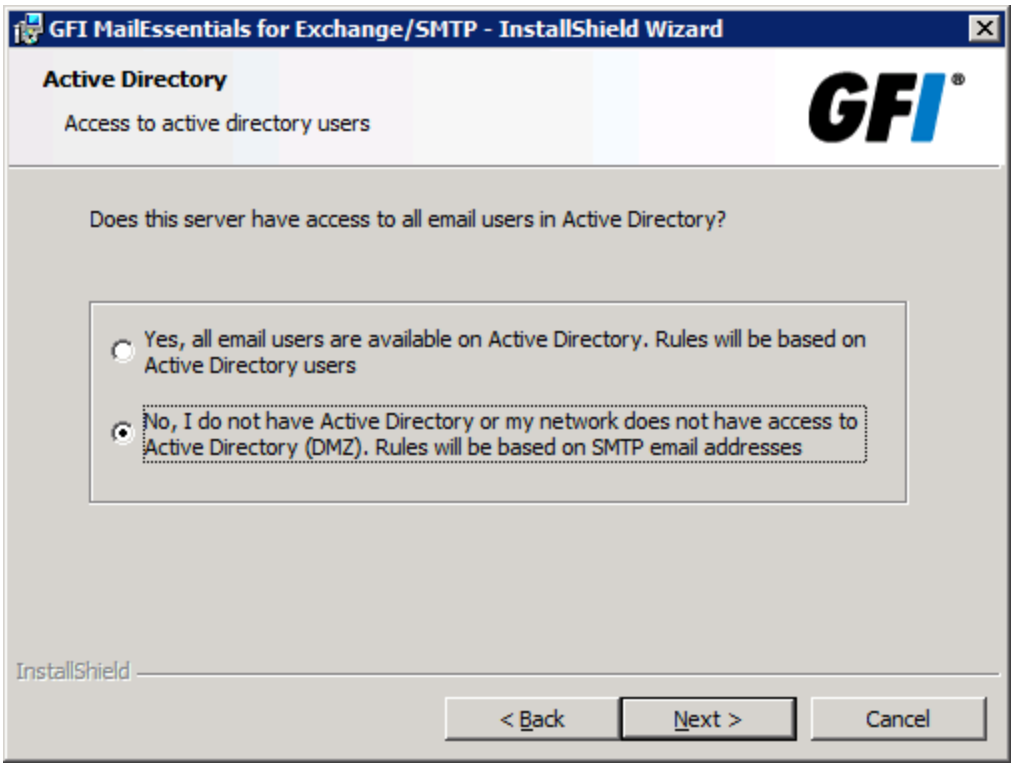
Use the information in this section to install and configure Lotus Domino with GFI MailEssentials. Install GFI MailEssentials on a separate machine then Lotus Domino, as seen on the figure below.

Figure 4: GFI MailEssentials installation on a separate server than Lotus Domino

15.2.1 Installing GFI MailEssentials

Install GFI MailEssentials by running the GFI MailEssentials installation file and following the onscreen instructions. For more information, refer to Installation (page 24).

If GFI MailEssentials is installed on a machine where Active Directory is present, one may encounter the dialog box below. Select **No, I do not have Active Directory…** to install GFI MailEssentials in SMTP mode.


GFI MailEssentials for Exchange/SMTP - InstallShield Wizard
Active Directory
Access to active directory users
GFI
Does this server have access to all email users in Active Directory?
Yes, all email users are available on Active Directory. Rules will be based on Active Directory users
No, I do not have Active Directory or my network does not have access to Active Directory (DMZ). Rules will be based on SMTP email addresses
InstallShield
< Back
Next >
Cancel

Screenshot 151: Active Directory selection

15.2.2 Set up DNS/Router Firewall

Configure the machine where GFI MailEssentials is installed to act as a gateway (also known as "Smart host" or "Mail relay" server) for all email. Effectively, all inbound email must pass through this machine before relayed to the mail server for distribution (it is the first to receive all emails destined for your mail server).

The same applies for outbound emails; mail server must relay all outgoing emails to the gateway machine for scanning before these are sent to external recipients via Internet (it must be the last 'stop' for emails destined for the Internet). In this way, GFI MailEssentials checks all inbound and outbound mail it is delivered to the recipients.

The MX record of your domain must point to the mail relay server

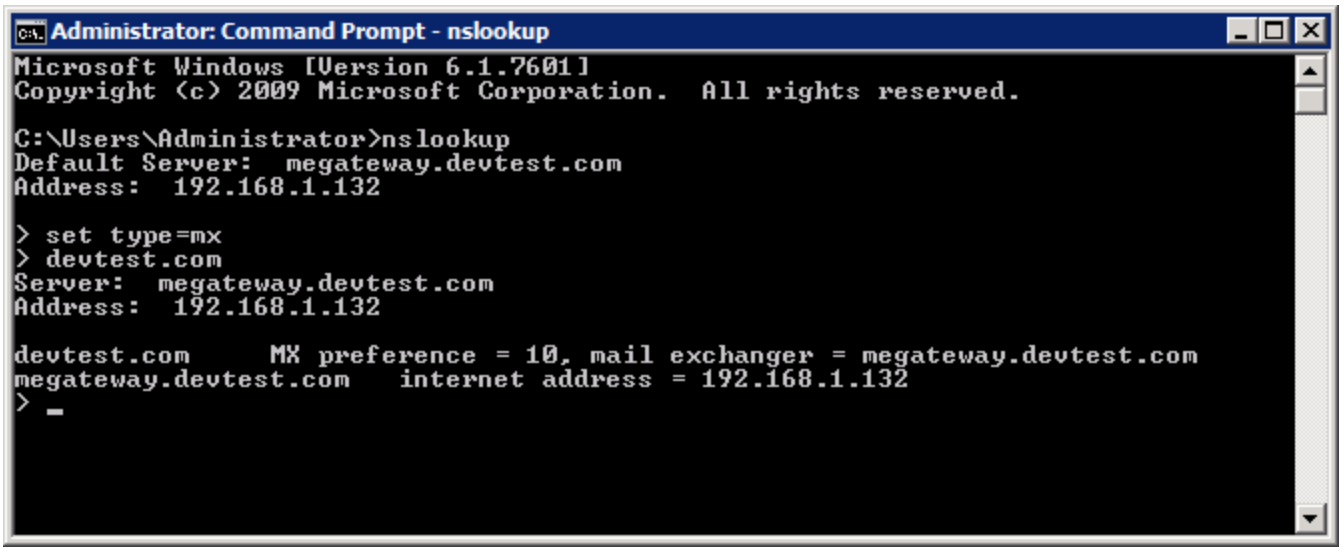
> **NOTE**
>
> If your ISP manages the DNS server, ask this provider to update it for you.

Since the new mail relay server must first receive all inbound email, update the MX record of your domain to point to the IP of the new mail relay/Gateway server.

Verify the MX record of your DNS server as follows:

1. From command prompt, type `nslookup` and press **Enter**.
2. Type `set type=mx` and press **Enter**.
3. Type your mail domain and press **Enter**.

The MX record should return a single IP that corresponds to the IP address of the machine running GFI MailEssentials.



Screenshot 152: Verifying the MX record of the DNS

4. Test the new mail relay server. Before proceeding to install GFI MailEssentials, verify that the new mail relay server is working correctly.
5. Test the IIS SMTP inbound connection of the mail relay server by sending an email from an external account to an internal user (use web-mail, for example MSN Hotmail,if you do not have an external account available). Verify that the email client received the email.
6. Test the IIS SMTP outbound connection of your mail relay server by sending an email to an external account from an email client. Verify that the external user received the email.

> **NOTE**
>
> Alternatively, instead of an email client, send email manually through Telnet. This will give you more troubleshooting information.

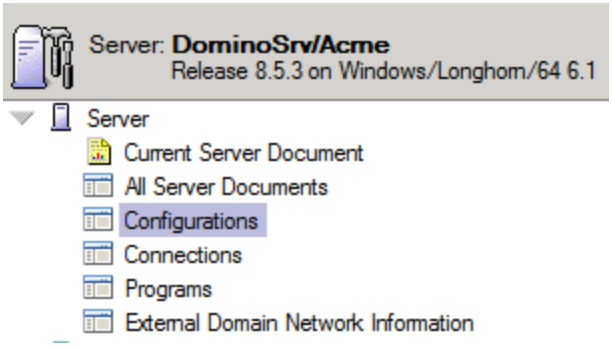
For more information, refer to:

http://support.microsoft.com/support/kb/articles/Q153/1/19.asp

15.2.3 Configuring Lotus Domino to send outbound emails through GFI MailEssentials

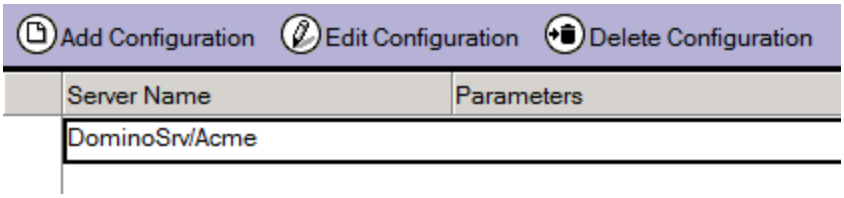
To direct all outgoing emails to the server where GFI MailEssentials is installed, Lotus Domino needs to be configured as below.

1. From the Lotus Domino Administrator, click **Configuration** tab and select **Server > Configurations**.



Screenshot 153: Lotus Domino Administrator - click Configurations option.

2. After configuration section is selected, main window will show the configuration of the server. Select desired server and click **Edit configuration**.

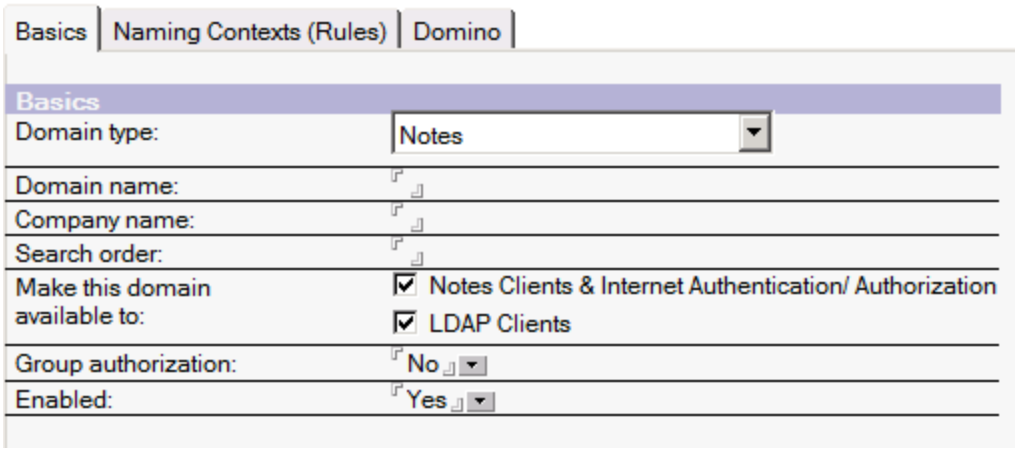


Screenshot 154: Click Edit Configuration

From the configuration document page, select **Router/SMTP** tab and ensure that **Basics** is selected. Double click on content to enable edit mode. Select **Relay host for messages leaving the local internet domain** and enter the IP Address of the machine that GFI MailEssentials is installed. Click **Save and Close** to save configuration document.

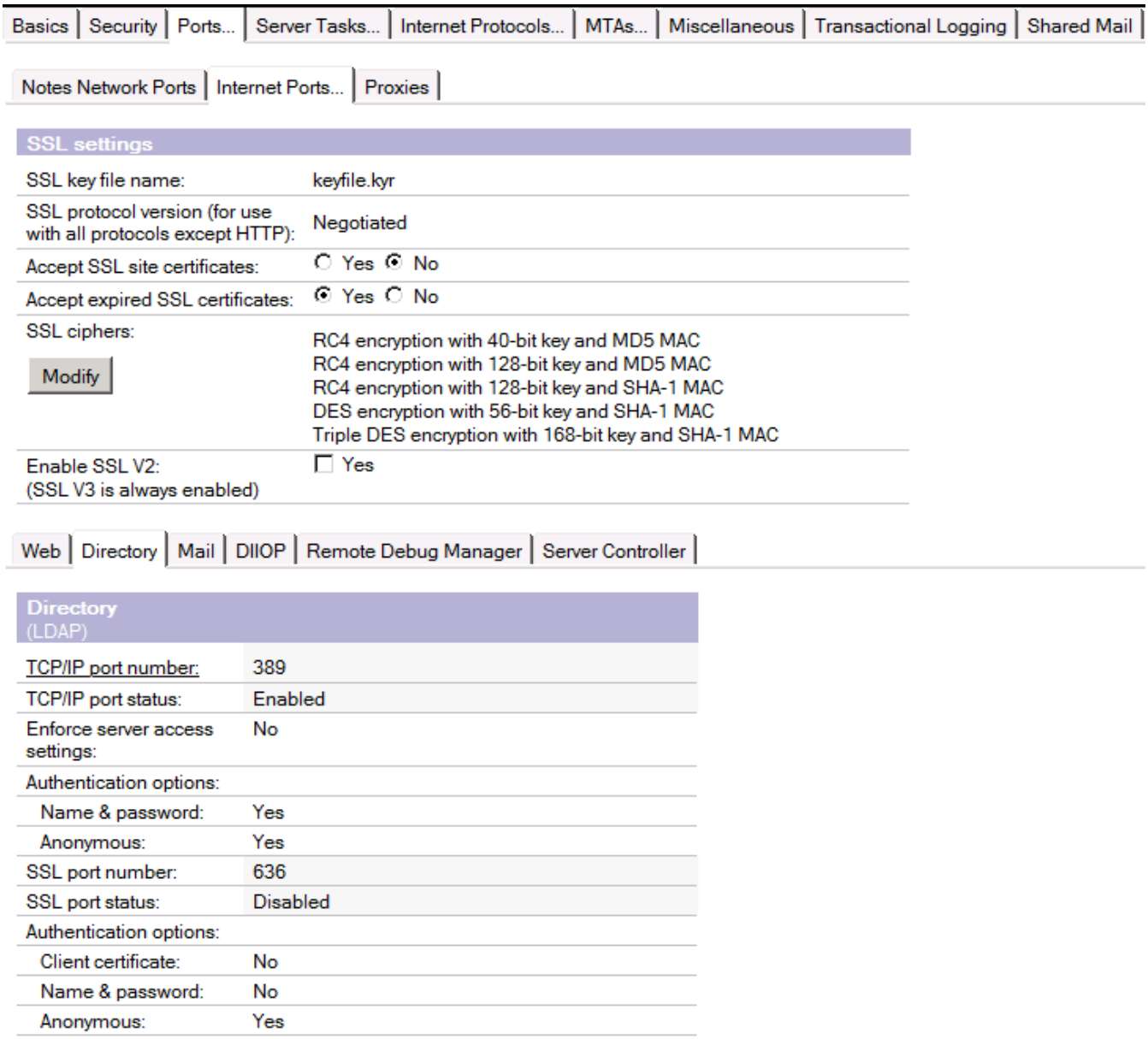
15.2.4 Lotus Domino LDAP Settings

From Lotus Domino, enable Directory Catalog and Directory Assistance. In the Directory Assistance database, click **Add Directory Assistance** to create a new Assistance document. In the document, one must enable the LDAP clients under **Make this domain available to** as follows:-



Screenshot 155: Lotus Domino LDAP Settings

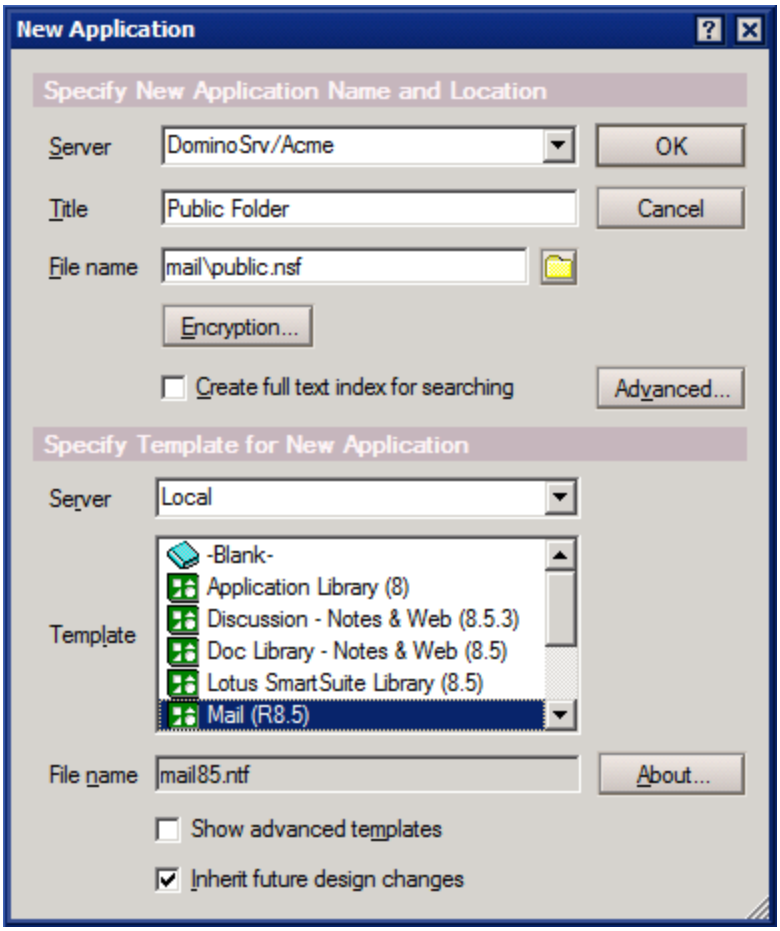
In the server configuration one must edit the credentials under the configuration. Anonymous authentication must be enabled so that GFI MailEssentials can access the Lotus Domino LDAP.



Screenshot 156: Enable Anonymous Authentication

15.3 Lotus Domino Anti Spam Folder Configuration

1. From Lotus Notes Administrator, create a database with the normal MAIL85.NTF template, that is used as the public folder. When the database is created, right click the database from the files section and select **Access Control**. Configure the user or group or server to have access on the database.



Screenshot 157: Create a new database

2. Convert the database using the server console by typing:

```
load convert -e -h mail\public.nsf
```

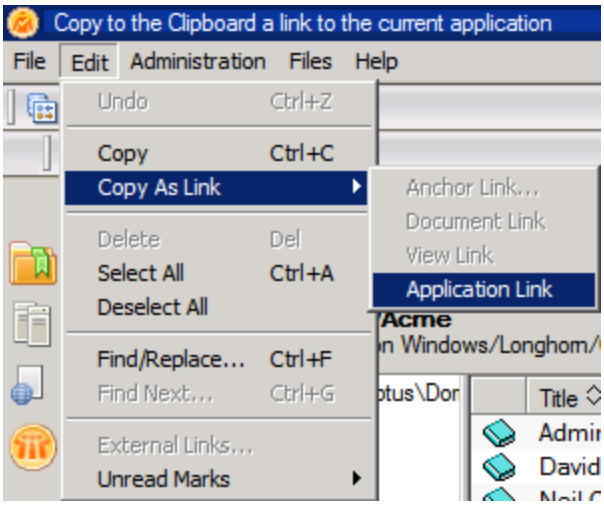
Command should display the following results.

```
load convert -e -h mail\public.nsf

[0A34:0002-06F4] 19/09/2012 16:48:43   Mail Conversion Utility starting
[0A34:0002-06F4] 19/09/2012 16:48:43   Mail Convert: Started enabling NSF support for IMAP
in 'mail\public.nsf'
[0A34:0002-06F4] 19/09/2012 16:48:43   Mail Convert: Finished enabling NSF support for IMAP
in 'mail\public.nsf'
[0A34:0002-06F4] 19/09/2012 16:48:43   Mail Convert: Started adding IMAP specific items in
'mail\public.nsf'
[0A34:0002-06F4] 19/09/2012 16:48:43   Mail Convert: Finished adding IMAP specific items in
'mail\public.nsf'. 0 messages succeeded, 0 messages failed.
[0A34:0002-06F4] 19/09/2012 16:48:43   Mail Conversion Utility shutdown
```

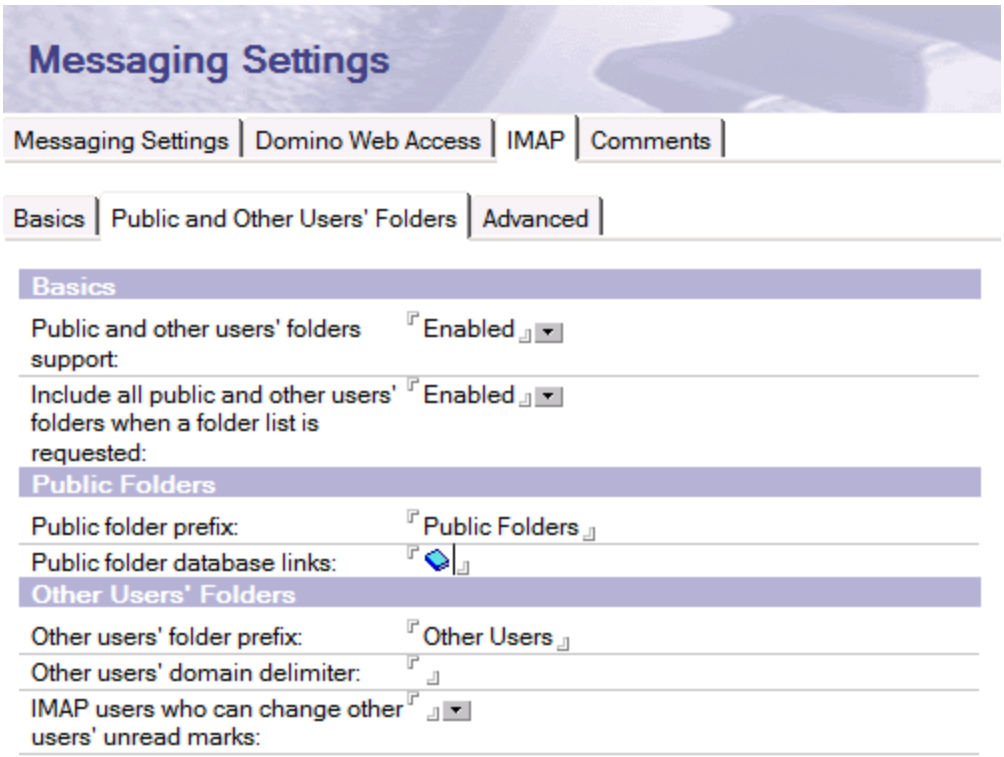
Screenshot 158: Load convert result

3. On completion, ensure that the database is accessible from IMAP service. From the Lotus Notes Administrator, go to **Configuration**, and select the **Files** tab. Highlight the database of the public folder, click **Edit**, select **Copy as Link** and click **Application Link**.



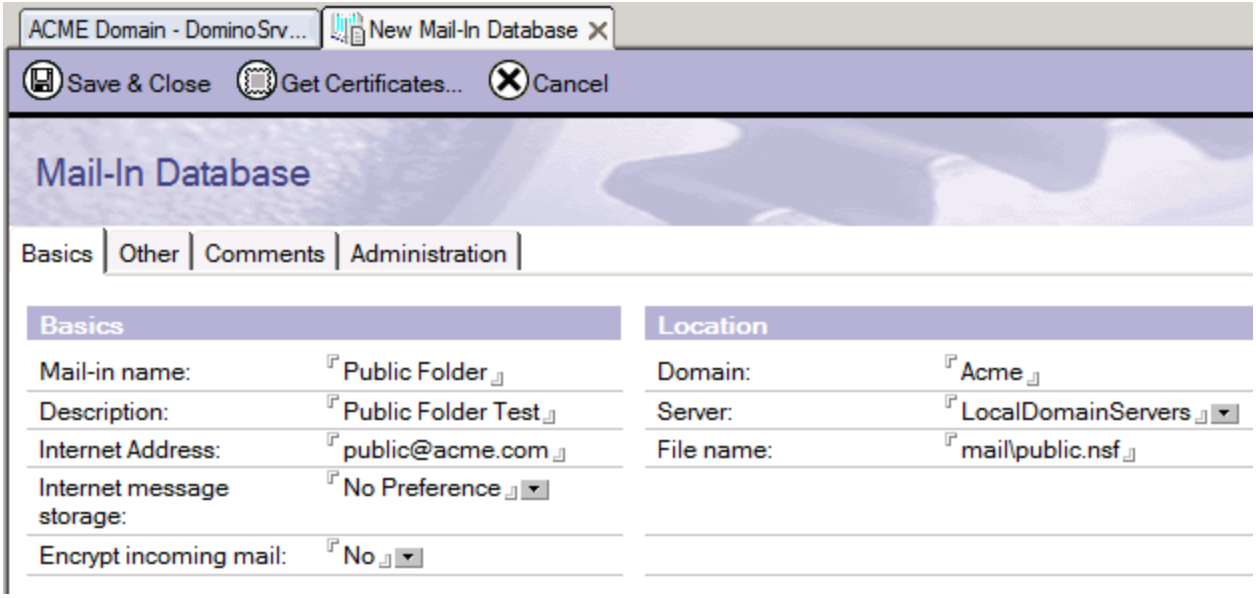
Screenshot 159: Copy to the clipboard a link to the current application

4. From the configuration, go to **Messaging Settings** and select **IMAP** tab.



Screenshot 160: Include all public and other users' folders when a folder list is requested

5. Select **Public and Other Users' Folders** tab. Right click and paste on the **Public Folders Database Links** and enable the **Include all public and other users folders when a folder list is requested'**.
6. Save and close the document.



Screenshot 161: New mail-in database

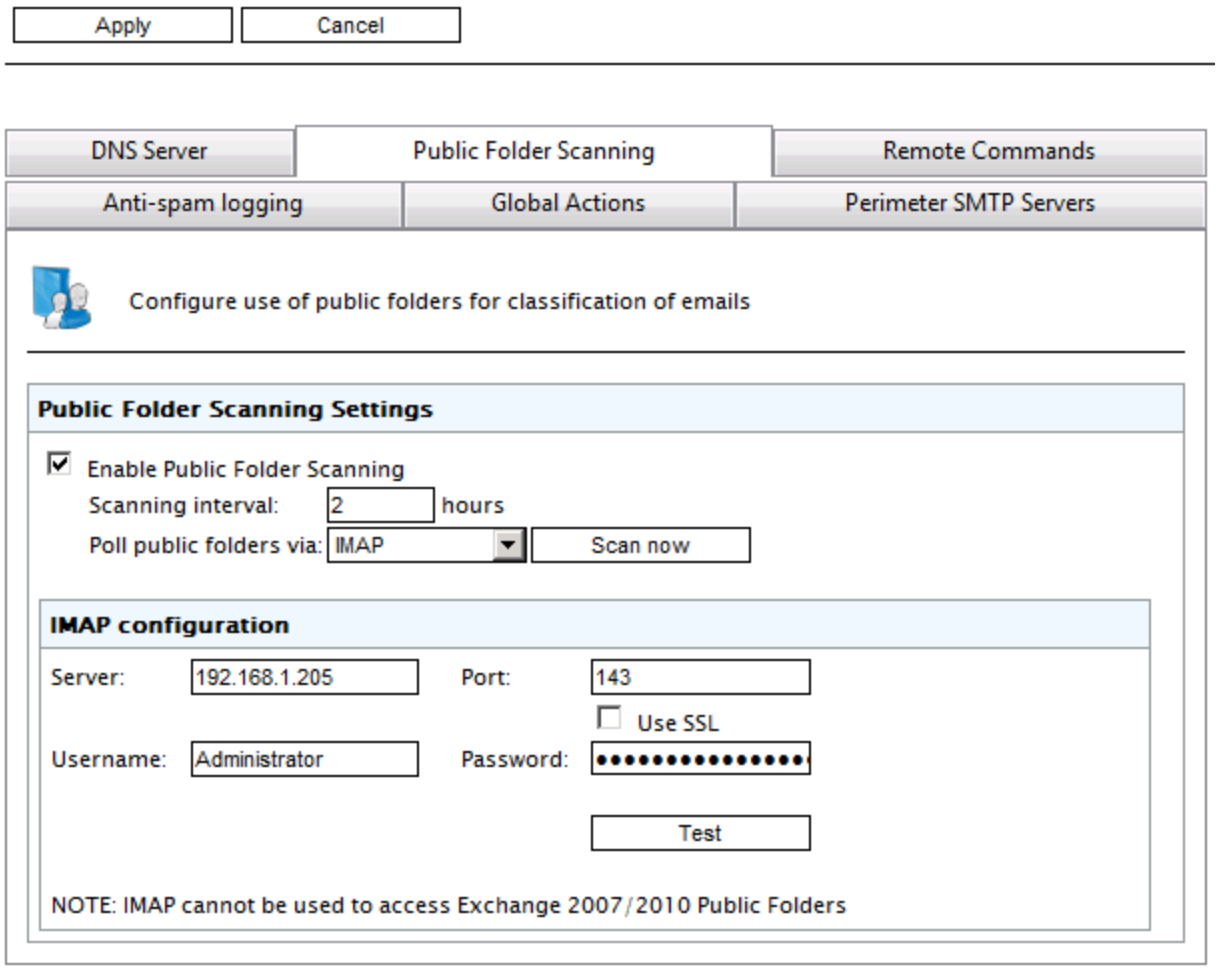
7. From the Lotus Notes Administrator, configure the folder for mail usage. Go to **People and Groups** and select **Mail-In Database**. Create a new Mail-in Database and in the whole directory path enter the full path (for example, Mail\public.nsf).
8. Save and close the document.

15.4 GFI MailEssentials Configuration

1. From the GFI MailEssentials web interface, expand **AntiSpam** and select **AntiSpam Settings**.
2. On the right hand pane, select **Public Folder Scanning** tab and enable **Public Folder Scanning**.
3. From the **IMAP configuration** section, enter the IMAP server (your Lotus Domino server, Port and the credentials of the user to access the folder).

> **NOTE**
>
> The test button will not function.

4. Click **Apply** to save modifications.



Screenshot 162: Enable Public Folder Scanning

5. From the registry , change values to use this function. From the registry select `HKEY_LOCAL_MACHINE\SOFTWARE\GFI\ME12\ATTENDANT\RPFOLDERS:5` and create the following Key String Value as follows:

```
Name/Value
SharedNamespace Public Folders\\Public Folder
FolderDelimiter \\
```

16 Appendix 3 - Microsoft® Exchange 2003 Clusters

Use this appendix for instructions on how to install and uninstall GFI MailEssentials on Microsoft® Exchange 2003 clusters.

A cluster is a group of servers, technically known as nodes, working collectively as a single server. Such environment provides high availability and fail over mechanisms to ensure constant availability of resources and applications including email infrastructures. If one of the nodes in the cluster fails/is not available, resources and applications switch to another cluster node.

NOTE

GFI MailEssentials can only be installed in an Active-Passive cluster environment. In an active/passive cluster, a 'failover' mechanism ensures that whenever an active cluster fails, one of the available passive nodes becomes active (i.e. takes over the role of the failed node).

16.1 Installing GFI MailEssentials in a cluster environment

To install GFI MailEssentials on a Microsoft® Exchange Server 2000/2003 cluster ensure that:

- Any running applications are closed.
- Microsoft® Exchange Server 2000/2003 is installed in clustered mode.
- An Exchange Virtual Server cluster group resource exists and includes, among other things, a Physical Disk cluster resource.
- All cluster nodes should be turned off, except the node where GFI MailEssentials will first be installed.

1. Start the installation process and ensure that:
   - All files are installed on the shared hard drive
   - You are installing on the machine's Default Website
2. On completion, start default website using IIS Manager.
3. Go to **Control Panel > Administrative Tools > Cluster Administrator** and create a new resource group (Right click **Groups > New > Group**).
4. Key in `GFI MailEssentials` as the name and `Services for GFI MailEssentials` as the description. Click **Next**.
5. Move all available nodes to **Preferred Owners** and click **Finish**.
6. Right click **GFI MailEssentials > New > Resource**.
7. Set the name as `GFI List Server`.
8. Set Resource Type to Generic Service and click **Next**.
9. Set all available nodes to possible owners and click **Next**.
10. Click **Next**.
11. Set service name to `listserv` and click next.

12. Click **Finish**.
13. Repeat steps 7 to 12 with the following details:

Name	Service Name
GFI MailEssentials AntiSpam Attendant	gfiasmlhost
GFI MailEssentials AS Scan Engine	gfiscans
GFI MailEssentials Autoupdater	msecavupdate
GFI MailEssentials AV Scan Engine	gfiscanm
GFI MailEssentials EmailSecurity Attendant	msecmlhost
GFI MailEssentials Enterprise Transfer	gfimetrxsvc
GFI MailEssentials Legacy Attendant	gfiasmsecatt
GFI MailEssentials LocalMode Host	csecmlhost
GFI POP2Exchange	gfipop2exch

14. On completion, bring the GFI MailEssentials group online.
15. Shut down this node and start a new node.
16. Repeat steps 1 and 2 for all cluster nodes.

16.2 Uninstalling GFI MailEssentials in a cluster enviornment

Ensure that only only one cluster node is turned on; the rest should all be turned off.

1. Stop all GFI services
2. Backup all the contents of theGFI MailEssentials installation folder to a different location.
3. Delete all GFI Services from the Cluster Resources from the group GFI MailEssentials.
4. Start all GFI services and ensure all cluster services and Exchange services are up and running.
5. Uninstall from first Node.
6. From command prompt
   - Type `sc delete msecavupdate` and press **Enter**.
   - Type `sc delete gfiasmsecatt` and press **Enter**.
7. Click **Start > Run** and type `regedit`. Press **Enter**.
8. Locate and delete the `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\GFI` key
9. Copy the backup of GFI MailEssentials to where it was installed.
10. Turn off the current node and start the next node. Ensure all cluster services, Exchange services and GFI MailEssentials services are up and running
11. Uninstall GFI MailEssentials.
12. From command prompt:
    - Type `sc delete msecavupdate` and press **Enter**.
    - Type `sc delete gfiasmsecatt` and press **Enter**.
13. Repeat steps 7 to 12 for all remaining nodes.
14. Delete the GFI MailEssentials installation folder and its backup. From cluster administrator delete all GFI services.

17 Glossary

A

Active Directory
A technology that provides a variety of network services, including LDAP directory services.

AD
See Active Directory

Anti-virus software
Software that detects malware such as Trojan horses in emails, files and applications.

Auto-reply
An email reply that is sent automatically to incoming emails.

B

Background Intelligent Transfer Service
A component of Microsoft Windows operating systems that facilitates transfer of files between systems using idle network bandwidth.

Bayesian Filtering
An anti-spam technique where a statistical probability index based on training from users is used to identify spam.

BITS
See Background Intelligent Transfer Service

Blocklist
A list of email addresses or domains from whom email is not to be received by users

Botnet
A network of infected computers that run autonomously and are controlled by a hacker/cracker.

C

CIDR
See Classless Inter-Domain Routing

Classless Inter-Domain Routing
An IP addressing notation that defines a range of IP addresses.

D

Decompression engine

A scanning module that decompresses and analyzes archives (for example, .zip and .rar files) attached to an email.

Demilitarized Zone

An internet-facing section of a network that is not part of the internal network. Its purpose typically is to act as a gateway between internal networks and the internet.

Directory harvesting

Email attacks where known email addresses are used as a template to create other email addresses.

Disclaimer

A statement intended to identify or limit the range of rights and obligations for email recipients

DMZ

See Demilitarized Zone

DNS

See Domain Name System

DNS MX

See Mail Exchange

Domain Name System

A database used by TCP/IP networks that enables the translation of hostnames to IP addresses and provides other domain related information.

E

Email headers

Information that precedes the email text (body) within an email message. This includes the sender, recipient, subject, sending and receiving time stamps, etc.

Email monitoring rules

Rules which enable the replication of emails between email addresses.

Exploit

An attack method that uses known vulnerabilities in applications or operating systems to compromise the security of a system.

F

False negatives

Spam emails that are not detected as spam.

False positives

Legitimate emails that are incorrectly identified as spam.

G

Gateway

The computer (server) in a LAN that is directly connected to an external network. In GFI MailSecurity, gateway refers to the email servers within the company that first receive email from external domains.

Greylist filter

An anti-spam filter that blocks emails sent from spammers that do not resend a message when a retry message is received.

H

Ham

Legitimate e-mail

HTML Sanitizer

A filtering module within GFI MailSecurity that scans and removes html scripting code from emails.

HTTP

Hypertext Transfer Protocol - A protocol used to transfer hypertext data between servers and internet browsers.

I

IIS

See Internet Information Services

IMAP

See Internet Message Access Protocol

Internet Information Services

A set of Internet-based services created by Microsoft Corporation for internet servers.

Internet Message Access Protocol

One of the two most commonly used Internet standard protocols for e-mail retrieval, the other being POP3.

L

LDAP

See Lightweight Directory Access Protocol

Lightweight Directory Access Protocol

An application protocol used to query and modify directory services running over TCP/IP.

List server

A server that distributes emails sent to discussions lists and newsletter lists, and manages subscription requests.

M

Mail Exchange

The DNS record used to identify the IP addresses of the domain's mail servers.

Malware

All malicious types of software that are designed to compromise computer security and which usually spread through malicious methods.

MAPI

See Messaging Application Programming Interface

MDAC

See Microsoft Data Access Components

Messaging Application Programming Interface

A messaging architecture and a Component Object Model based API for Microsoft Exchange.

Microsoft Data Access Components

A Microsoft technology that gives developers a homogeneous and consistent way of developing software that can access almost any data store.

Microsoft Message Queuing Services

A message queue implementation for Windows Server operating systems.

MIME

See Multipurpose Internet Mail Extensions

MSMQ

See Microsoft Message Queuing Services

Multipurpose Internet Mail Extensions

A standard that extends the format of e-mail to support text other than ASCII, non-text attachments, message bodies with multiple parts and header information in non-ASCII character sets.

N

NDR

See Non Delivery Report

Non Delivery Report

An automated electronic mail message sent to the sender on an email delivery problem.

P

Perimeter server/gateway

The host in a LAN that is directly connected to an external network. In GFI MailEssentials perimeter gateway refers to the email servers within the company that first receive email from external domains.

PGP encryption

A public-key cryptosystem often used to encrypt emails.

Phishing

The process of acquiring sensitive personal information with the aim of defrauding individuals, typically through the use of fake communications

POP2Exchange

A system that collects email messages from POP3 mailboxes and routes them to mail server.

POP3

See Post Office Protocol ver.3

Post Office Protocol ver.3

A client/server protocol for storing emails so that clients can connect to the POP3 server at any time and read the email. A mail client makes a TCP/IP connection with the server and by exchanging a series of commands, enable users to read the email.

Public folder

A common folder that allows Microsoft Exchange user to share information.

Q

Quarantine

A email database where emails detected as spam and/or malware are stored in a controlled enviornment. Quarantined emails are not a threat to the network enviorment.

Quarantine Store

A central repository within GFI MailSecurity where all blocked emails are retained until they are reviewed by an administrator.

R

RBL

See Realtime Blocklist

Realtime Blocklist

Online databases of spam IP addresses. Incoming emails are compared to these lists to determine if they are originating from blocked users.

Recursive archives

Archives that contain multiple levels of sub-archives (that is, archives within archives). Also known as nested archives.

Remote commands

Instructions that facilitate the possibility of executing tasks remotely.

RSS feeds

A protocol used by websites to distribute content (feeds) that frequently changes (for example news items) with its subscribers.

S

Secure Sockets Layer

A protocol to ensure an integral and secure communication between networks.

Simple Mail Transport Protocol

An internet standard used for email transmission across IP networks.

SMTP

See Simple Mail Transport Protocol

Spam actions

Actions taken on spam emails received, e.g. delete email or send to Junk email folder.

SSL

See Secure Sockets Layer

T

Trojan horse

Malicious software that compromises a computer by disguising itself as legitimate software.

V

Virus scanning engine

A virus detection technology implemented within antivirus software that is responsible for the actual detection of viruses.

W

WebDAV

An extension of HTTP that enables users to manage files remotely and interactively. Used for managing emails in the mailbox and in the public folder in Microsoft Exchange.

Whitelist

A list of email addresses and domains from which emails are always received

Z

Zombie

An infected computer that is made part of a Botnet through malware.

18 Index

A

Active Directory 20, 28, 34, 42, 62, 65, 102, 107, 151, 197, 202, 223, 241, 249, 251, 269

Antispam 51, 149, 238

Antivirus 19, 26-27, 32, 51, 68-69, 73, 77, 81, 85, 89, 177, 188

Attachment Filtering 19, 163, 179, 220, 223

Auto-replies 15-16, 18, 205

B

Bayesian Analysis 20, 27, 102, 128, 145, 220, 262, 266

C

Cluster 26

D

Dashboard 14, 45-46, 49, 51-52, 260

Database 20, 45, 47, 52, 57-58, 91, 102, 105, 110, 119, 129, 146, 209, 211, 223, 261-262, 265, 272-273

DEP 42

Directory harvesting 18, 20, 23, 42, 102, 107, 220, 249, 251

Disclaimers 15-16, 201, 263

DMZ 22, 28, 34, 151, 198

DNS Server 31, 36, 113, 123, 144, 270

Domain 14, 19, 34, 107, 113, 116-117, 123, 130, 150, 198, 202, 206, 209, 217, 223, 225, 241, 243, 260, 269-270

E

Edge Server 21, 28

Email Blocklist 20, 102, 110-111, 145, 155, 220, 262

Email Direction 54, 56

Email monitoring 15, 18-19, 215, 263

F

firewall 22, 27, 32, 108, 198, 262, 270

G

gateway 21, 25-26, 28, 33, 69, 72, 76, 80, 85, 115, 183, 189, 232, 260, 263, 270

Greylist 20, 42, 102, 119, 220

H

Header checking 20, 102, 121

Hub Transport 16, 21, 28, 88

I

IIS 23, 25, 28, 33, 62, 119, 199, 222-223, 226-227, 242, 248, 250, 260, 262, 271, 278

IMAP 150, 260, 274

Inbound mail filtering 18

Internal email 31, 44

Internet 18, 25, 29, 37, 148, 221, 237, 242, 262, 267, 270

IP 30, 36, 60, 98, 112, 115, 117, 119, 123, 133, 198, 220-221, 235, 262, 265, 270

IP DNS Blocklist 20, 27, 102, 138, 144

ISP 237, 270

K

Kaspersky 19, 42, 68, 76

Keyword checking 20, 102, 124, 145

L

LDAP lookups 198

Legitimate email 20, 42, 102, 128, 130

Licensing 15, 40, 223, 261

Lotus Domino 21, 28, 31, 150, 269, 273

Lotus Notes 31, 273

M

MAPI 150, 239

Microsoft Exchange 40, 232, 240

MSMQ 26

N

New Senders 18, 20, 102, 134, 137-138, 220

Newsletter 208, 211

O

Outbound mail filtering 18

P

Performance 30, 42, 132, 225, 233, 255, 265

perimeter server 22, 28, 99, 119

Phishing 20, 27, 40, 101, 105, 220, 239

POP2Exchange 16, 45, 52, 235, 248, 250, 279

POP3 31, 235, 260

Post-Installation 35-36, 249, 251

Q

Quarantine 19, 35, 39, 44, 47, 62, 64, 70, 74, 77, 82, 86, 91, 95, 136, 160, 166, 171, 175, 180, 190, 192, 198, 220, 226-228, 261

R

Remote commands 18, 145, 261

RSS Feeds 35, 190, 226

S

Sender Policy Framework 20, 102, 115, 262

SMTP Server 28, 34, 40, 118-119, 148, 260

SMTP Virtual Server 29, 35, 223

Spam actions 135, 247, 251

SpamRazer 20, 27, 101-102, 135, 220, 262

U

Updates 27, 45, 51, 68, 71, 75, 78, 83, 87, 93, 96, 102, 106, 129, 221, 225, 246, 260

Upgrade 40

URI DNS Blocklist 20, 102, 114

V

VIPRE Email Security for Exchange 32

Virtual directory 17, 35, 150, 227-228, 242

W

WebDAV 150

Whitelist 19-20, 62, 98, 102-103, 111, 115, 117, 123, 130, 133-134, 145, 149, 154, 220, 262

Wizard 29, 32, 36, 41, 115, 130, 210, 222, 243, 266

USA, CANADA AND CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104 Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

ENGLAND AND IRELAND

Magna House, 18-32 London Road, Staines, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.com

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com

GFI®